UNIVERSIDAD NACIONAL DE TUCUMÁN

FACULTAD DE CIENCIAS ECONOMICAS
UNIVERSIDAD NACIONAL TUCUMAN

SEGURIDAD DE SMARTPHONES EN ENTORNOS EMPRESARIALES

Autores: Chico Costas, Alejo Martín
Cuadra, Alexia Magalí
Durán, Natalia Giselle

Director: La Marca, Marcelo

2013

Trabajo de Seminario: Licenciatura en Administración de empresas

ABSTRACT

Los sistemas y tecnologías de la Información son vitales dentro de las organizaciones, y los cambios que producen obligan a las empresas a adaptarse. Los *Smartphones* son utilizados cada vez con mayor frecuencia en entornos empresariales, proporcionando información oportuna en el momento oportuno.

La introducción de los teléfonos inteligentes en las organizaciones implica nuevas consideraciones en lo que respecta a la seguridad de la información. La posibilidad de utilizar distintas redes de conexión y aplicaciones de diversa índole y de transportar el dispositivo, contribuyen a que el trabajo sea cada vez más móvil. Además, el trabajo en la nube o *Cloud Computing* permite prescindir de computadoras y servidores propios, posibilitando el acceso a los sistemas desde cualquier *Smartphone* y en cualquier momento.

Siendo la información el capital más importante con el que cuentan las organizaciones, existe un factor de gran relevancia a la hora de adoptar los dispositivos inteligentes: la seguridad.

Para contribuir a una gestión segura, productiva y móvil, sacando el mayor provecho posible a las últimas tecnologías, en el presente trabajo se analizan las vulnerabilidades, riesgos y peligros implicados en la implementación de *Smartphones* en entornos empresariales. También se recopilan recomendaciones que deber ser tenidas en cuenta por los usuarios y se analizan las prácticas de seguridad de la información contenidas en la ISO 27000:2005.

Por último, para ejemplificar la aplicación de las consideraciones mencionadas, se exponen casos exitosos de soluciones empresariales basados en *Smartphones*, como las implementadas por BlackBerry para sus clientes.

PRÓLOGO

La presente Tesina se realizó como trabajo final para la materia Seminario de la Facultad de Ciencias Económicas de la Universidad Nacional de Tucumán.

Las nuevas Tecnologías de la Información introducen grandes cambios en los entornos corporativos, obligando a las empresas a adaptarse a los mismos para lograr una ventaja competitiva o, en algunos casos, para subsistir. Las ventajas que representan el uso empresarial de los Smartphones y la posibilidad de trabajar en la nube, han logrado su implementación en cada vez más empresas. Siendo la información el capital más importante con el que cuentan las organizaciones, existe un factor de gran relevancia a la hora de adoptar los dispositivos inteligentes: la seguridad.

Con este trabajo se pretende introducir al lector en las consideraciones generales a tener en cuenta al incorporar Smartphones a empresas de cualquier tamaño, poniendo especial énfasis en la seguridad de la información. Se desea contribuir a una gestión segura, productiva y móvil, sacando el mayor provecho posible a las últimas tecnologías. Con este fin, se muestran casos exitosos de implementación de los conceptos expuestos.

CAPÍTULO I

Tecnologías de Información

Sumario: 1. Las tecnologías de información en las empresas; 2. ¿Qué es un *Smartphone*?; 3. Prestaciones del *Smartphone*; 4. Ventajas de los *Smartphones*; 5. Desventajas de los *Smartphones.*

1.- Las tecnologías de información en las empresas

Los sistemas y las tecnologías de información son un elemento vital de las organizaciones y negocios exitosos.

La tecnología de información puede a ayudar a todo tipo de negocios a mejorar la eficiencia y la efectividad de sus procesos de negocios, la toma gerencial de decisiones y la colaboración entre los grupos de trabajo, mediante el fortalecimiento de sus posiciones competitivas en un mercado rápidamente cambiante.[1]

Es necesario establecer que la tecnología de la información se entiende como aquellas herramientas y métodos empleados para recabar, retener, manipular o distribuir información. La tecnología de la información se

[1] O´BRIEN, James A y MARAKAS, George M, Sistemas de Información Gerencial, 7° Edición, Editorial Mc Graw-Hill, trad. por María Jesús Herrero Díaz, (México, 2006), pág. 4.

encuentra generalmente asociada con las computadoras y las tecnologías afines aplicadas a la toma de decisiones.

La tecnología de la información está cambiando la forma tradicional de hacer las cosas, las personas que trabajan en el gobierno, en empresas privadas, que dirigen personal o que trabajan como profesional en cualquier campo utilizan las tecnologías de información cotidianamente mediante el uso de Internet, las tarjetas de crédito, el pago electrónico de la nómina, entre otras funciones; es por eso que las funciones de las tecnologías de la información en los procesos de las empresas se han expandido a gran escala.

Las tecnologías de información representan una herramienta cada vez más importante en los negocios, sin embargo el implementar un sistema de información de una empresa no garantiza que esta obtenga resultados de manera inmediata o a largo plazo.[2]

A las tecnologías de la información muchas veces se las denomina nuevas tecnologías de la información y la comunicación, y son un concepto muy asociado a la informática. Si se entiende esta última como el conjunto de recursos, procedimientos y técnicas utilizadas en el procesamiento, almacenamiento y transmisión de información. Internet puede formar parte de ese procesamiento que, quizás, se realice de manera distribuida y remota. Y al hablar de procesamiento remoto, además de incorporar el concepto de telecomunicación, se puede estar haciendo referencia a un dispositivo muy distinto a lo que tradicionalmente se conoce por computadora pues podría llevarse a cabo, por ejemplo, con un teléfono móvil o una computadora ultraportátil, con capacidad de operar en red mediante comunicación inalámbrica y con cada vez más prestaciones, facilidades y rendimiento.

El éxito de un sistema de información no debería medirse solo por su eficiencia en términos de minimización de costos, tiempos y usos de los

---

[2] Consultas en Internet: www.tuobra.unam.mx (04/10/2013).

recursos de información. El éxito debería medirse también por la eficacia de la tecnología de información en el momento de apoyar las estrategias de negocios de una organización, con lo que hace posibles sus procesos de negocio, mejora sus estructuras y cultura organizacionales e incrementa el valor de los clientes y del negocio de la empresa.

Sin embargo, es importante darse cuenta de que la tecnología y los sistemas de información pueden ser mal administrados y mal aplicados, de forma tal que los problemas de desempeño de los sistemas de información llegan a crear fallas tecnológicas y de negocios.[3]

Las tecnologías de información conforman el conjunto de recursos necesarios para manipular la información y particularmente los ordenadores, programas informáticos y redes necesarias para convertirla, almacenarla, administrarla, transmitirla y encontrarla.

Se pueden agrupar las tecnologías de información de las comunicaciones en:

- Las Redes: Telefonía fija, banda ancha, telefonía móvil, redes de televisión, redes en el hogar. Este tema se verá con mayor profundidad en un capítulo posterior.
- Los Terminales: Computadoras personales, navegador de Internet, sistemas operativos para ordenadores, teléfono móvil, televisor, reproductores portátiles de audio y video, consolas de video juego.
- Los Servicios: Correo electrónico, búsqueda de información, banca on-line, audio y música, televisión y cine.

Entre las terminales mencionadas, los *smartphones* son los dispositivos cuyo uso se ha extendido con rapidez generando grandes cambios en las empre-

[3] O´BRIEN, James A y MARAKAS, George M. Op. Cit., pág 16.

sas. El desarrollo de la tecnología microelectrónica y de las redes de telecomunicación es lo que ha hecho posible su aparición y su popularización, de forma que son uno de los dispositivos tecnológicos multifunción más demandados en la actualidad por los usuarios.

2.- ¿Qué es un *Smartphone*?

Un *Smartphone* o teléfono inteligente es un término comercial para denominar a un teléfono móvil que ofrece más funciones que un teléfono móvil común.

La característica más importante de los *Smartphones* es que permite la instalación de programas para incrementar el procesamiento de datos y la conectividad. Estas aplicaciones pueden ser desarrolladas por el fabricante del dispositivo, por el operador o por un tercero.[4]

El *Smartphone* surge como resultado de la evolución de la tecnología celular. Un *Smartphone* es un teléfono móvil construido sobre una plataforma informática móvil, con una mayor capacidad de computación y conectividad que un teléfono móvil convencional. El término “inteligente” hace referencia a la capacidad de usarse como una computadora de bolsillo, llegando a remplazar a una computadora personal en algunos casos.[5]

Si bien hoy por hoy son muchas las compañías que lanzan teléfonos inteligentes a la venta, una es la que se destaca por sobre las demás por ser la precursora en la fabricación de éste tipo de equipos, este es el caso de la compañía estadounidense Apple que a través de iPhone, lidera el mercado de teléfonos celulares inteligentes, por encima de sus competidores directos BlackBerry, Nokia, LG o Samsung.

---

[4] Consultas en Internet: www.areatecnologia.com, (05/10/2013).
[5] Consultas en Internet: www.navactica.com, (05/10/2013).

3.- Prestaciones del *Smartphone*

Los *Smartphones* presentan una amplia gama de prestaciones que le aportan en sí, el atractivo que los caracteriza.

Estas prestaciones van desde las funciones ya incorporadas en los equipos anteriores como ser cámaras fotográficas y de video de mejor calidad y definición, hasta reproductores de música mp3.

Los *Smartphones* poseen funciones incorporadas que convierten a este tipo de teléfonos en una especie de computadoras personales pequeñas, como ser:

- Conexión a redes inalámbricas de Internet- wifi.
- Sistema operativo, como el de los ordenadores personales, pero adaptados a los equipos de telefonía celular.
- Aplicaciones del Sistema Operativo que cumplen la misma función que los programas de las computadoras convencionales. Y que sirven para cumplir con tareas específicas.
- Conexión bluetooth y 3G, y en las actualidad se ofrecen conexiones de hasta 4G.
- Pantalla táctil que facilita el acceso a las diferentes aplicaciones del teléfono.
- Tarjeta de memoria expandible, que amplía la capacidad de memoria por encima del que tiene un teléfono habitualmente.
- Acceso a las redes sociales. Como por ejemplo: Facebook o Twitter.
- Conectividad con las computadoras portátiles. Por ejemplo: Notebook.

- Navegación GPS.

4.- Ventajas de los *Smartphones*

Cuando una empresa decide invertir en tecnología, una alternativa es proporcionar a sus empleados teléfonos inteligentes. Si bien en un principio no se reconocerían grandes beneficios para la compañía, sin embargo proporcionan diversas ventajas en el funcionamiento cotidiano de una empresa.[6]

Es por ello que si tenemos que hablar de las ventajas de los teléfonos inteligentes podemos enumerar un sin fin de propiedades. A continuación vamos a detallar las más relevantes:

- Comunicación al instante: permite que los empleados puedan comunicarse en todo momento acortando las distancias y por distintos medios, tales como textos, correo electrónico, chat, video llamadas, entre otras. Se logra una comunicación al instante y efectiva.
- Facilidad de apuntes: estos dispositivos móviles permiten tomar notas, realizar apuntes sin necesidad de recurrir a hojas sueltas, luego se puede acceder fácilmente a los archivos generados.
- Apoyo operacional: una empresa puede adaptar distintas aplicaciones a las tareas cotidianas de manera que resulten más eficientes y a un bajo costo permitiendo utilizar de Excel, Word, crear documentos PDF entre otras. De esta manera, se podrá aumentar la productividad del trabajo, al dar un soporte tecnológico inalámbrico a las distintas áreas funcionales de la empresa.

---

[6] Consultas en Internet: www.altonivel.com.mx, (10/10/2013).

- Accesibilidad: toda la información está centrada en un solo dispositivo, evitando tener que recurrir a otros celulares.
- Usos: pueden ser usados también como módem *bluetooth*, evitando el uso de cables. Siendo útil para quien use una *notebook* y desea tener acceso a Internet en salas de espera, restaurantes, aeropuertos, hospitales, etc. La conexión puede establecerse sin la necesidad de sacar el Smartphone del bolsillo.
- Ubicación: los Smartphones son de gran utilidad cuando se realizan reuniones de trabajo en otras ciudades o en distintos puntos de la ciudad, permitiendo la fácil localización de los mismos, indicando el lugar exacto, y trazando rutas y sus coordenadas exactas. Permitiendo llegar puntualmente a lugares importantes y a la vez se hace un uso efectivo del tiempo.
- Programas: los *Smartphones* tienen la ventaja de instalar y correr infinidad de aplicaciones y programas. Esto permite que los usuarios personalicen su dispositivo con programas para sus necesidades y preferencias personales. Además, existen numerosas aplicaciones que se pueden obtener de manera gratuita.
- Imagen: la imagen que proyecta un *Smartphone* puede favorecer a las empresas. Hoy en día, incluso los estudiantes cuentan con dispositivos de última generación, ya sea por moda, comodidad o para ayudarlos en sus labores de estudio. Entrar a una reunión importante con un celular antiguo saltará a la vista. “Dime que tecnología usas y te diré quién eres” podría ser el refrán del futuro, cuando cada vez cobren mayor relevancia los accesorios tecnológicos en la imagen que proyectamos.

5.- Desventajas de los *Smartphones*

Como dispositivo móvil novedoso, el *Smartphone* captura el mercado con todas las experiencias que propone a sus usuarios, sin embargo, debemos destacar las desventajas quizás más importantes que pueden surgir durante su uso:

- La mayor desventaja es la probabilidad de robo o extravío del *Smartphone*, debido a que en él se encuentra toda la información personal y confidencial de la empresa, clientes y hasta de proveedores. Si el dispositivo cayera en manos indebidas el perjuicio podría ser costoso.
- Es vulnerable a los virus y ataques al Sistema Operativo, tal como sucede en la actualidad con las computadoras portátiles o de escritorio.
- Otra desventaja de un *Smartphone* es el tema de la batería, puesto que es muy delicado ya no suelen tener mucha durabilidad. Usándolo gradualmente, la batería de un *Smartphone* dura un día entero aproximadamente. Esto varía obviamente según los modelos.
- El tiempo excesivamente largo que pueden llegar a tardar en arrancar algunos *Smartphones*, son quejas frecuentes de los usuarios.
- En cuanto a las pantallas de estos teléfonos, las mismas poseen la particularidad de ser muy pequeñas, lo cual dificulta la lectura de la información mostrada, a su vez cuando se expone ante mucha iluminación exterior tienden a dificultar la lectura.

- Finalmente, una desventaja no tan importante pero igualmente a tener en cuenta es que los *Smartphones* tienden a sobrecalentarse cuando se realizan muchas tareas que están relacionadas con archivos de contenidos multimedia (como ser reproducir videos). Es por ello la importancia del procesador.

CAPÍTULO II
Sistemas Operativos y Aplicaciones en los Smartphones

Sumario: 1. Sistemas operativos móviles; 2. Android; 3. iOS; 4. Blackberry OS; 5. Windows Phone; 6. Aplicaciones para *Smartphones*.

1. Sistemas operativos móviles

Un Sistema Operativo es un programa o conjunto de programas que efectúan la gestión de los procesos básicos de un sistema informático, y permite la normal ejecución del resto de las operaciones.[7]

Los *smartphones* o teléfonos inteligentes funcionan regidos por un sistema operativo (OS) móvil que tiene el mismo cometido que los sistemas operativos de los ordenadores. Gestionan y regulan el funcionamiento del aparato, aunque de un modo más simple.

Básicamente, un sistema operativo proporciona las funciones principales para el dispositivo electrónico, tales como el reconocimiento de entrada y la visualización de la interfaz de usuario dentro de la pantalla. Pero

[7] Diccionario de la Lengua Española, en Internet: www.lema.rae.es/drae, (15/10/2013).

además, dependiendo del sistema operativo que utilice el teléfono, también se verá afectada la rapidez y la fiabilidad de todos los procesos.

Actualmente, existen una enorme variedad de tipos de sistemas operativos para teléfonos móviles, y entre los OS más conocidos y populares nos encontramos con Android, iOS, BlackBerry OS y Windows Phone. Por lo general la mayoría de estos sistemas operativos se encuentran asociados con determinadas marcas de teléfonos, fabricados por empresas específicas. Otros teléfonos, en cambio, están disponibles para una variedad de plataformas.[8]

2. Android

Originalmente desarrollado por una organización independiente y basado en el sistema operativo Linux, el llamado Android OS es actualmente el sistema que comercializa la compañía Google para smartphones y tablets. Desde su creación y hasta la actualidad, se trata de un sistema operativo que continúa siendo de distribución libre y código abierto, lo que ha hecho que Android siga siendo elogiado por una enorme cantidad de usuarios, debido a su flexibilidad.

Tengamos en cuenta que cualquier persona puede desarrollar aplicaciones para Android, y cualquier empresa puede lanzar un teléfono o una tablet incluyéndolo como OS preinstalado. Por ello, una de las grandes ventajas que posee este sistema operativo radica en que actualmente existe una disponibilidad de miles y miles de aplicaciones gratuitas y de pago que los usuarios pueden aprovechar para optimizar el uso de su dispositivo con Android.

---

[8] Consultas en Internet: www.informatica-hoy.com.ar, (10/10/2013).

Asimismo, otro de los beneficios de esta plataforma radica en el hecho de que permite una excelente integración con todos los servicios brindados por Google, lo que amplía notablemente las posibilidades del sistema.

Además, al tratarse de un sistema de código abierto, permite que los usuarios realicen una personalización realmente profunda, ajustando la plataforma a sus necesidades y a los recursos del dispositivo en el que correrá Android.

Cabe destacar que además, los desarrolladores de Android ponen a disponibilidad de los usuarios una serie de actualizaciones frecuentes de la plataforma, las cuales por lo general no sólo reportan mejoras notables en el desenvolvimiento del software, sino que también le añaden nuevas características.

Entre los aspectos criticables de Android, por lo general muchos usuarios se quejan de la escasa oferta de juegos disponibles en Android Market, mientras que otros aseguran que una de las grandes contras de la plataforma reside en que muchas de las aplicaciones disponibles no se ajustan de forma adecuada a las pantallas de los dispositivos con Android.

3. iOS

El sistema operativo iOS de Apple, ha sido desarrollado para ser exclusivamente utilizado en los productos de la empresa, por lo que viene integrado a dispositivos tales como el iPhone, la brillante iPad y el iPod. Dos de los aspectos fundamentales de iOS están dados por la seguridad que posee este sistema operativo y la compatibilidad con los equipos mencionados.

Por supuesto, al tratarse de un producto creado por Apple para los dispositivos que la empresa fabrica y comercializa, se trata de una plataforma de código cerrado.

Entre las grandes ventajas que suelen señalar los usuarios de este sistema operativo, se destaca su facilidad de uso, ofreciendo una interfaz gráfica que permite un notable desempeño. Posee una gran performance en el ámbito multimedia, y al contrario de Android posee una gran variedad y calidad de juegos.

Entre sus defectos más notorios, en principio la principal desventaja radica en que sólo puede ser utilizado en productos Apple. Asimismo requiere un importante consumo de energía, lo que hace que la batería dure menos tiempo que en un dispositivo con Android.

Al tratarse de una plataforma de código cerrado, no permite la personalización profunda, por lo que los usuarios deben conformarse con un simple cambio de color y demás insignificancias. Además una de sus grandes desventajas es que se encuentra totalmente atado a iTunes; el reproductor de medios y tienda de contenidos multimedia desarrollado por Apple con el fin de reproducir, organizar y sincronizar iPods, iPhones, iPads y comprar música.

4. Blackberry OS

Uno de los sistemas operativos más conocidos dentro del mundo de los teléfonos móviles inteligentes es sin dudas el BlackBerry OS, y como su nombre lo indica, es el único sistema operativo disponible para los dispositivos de la marca BlackBerry.

Debido a que fundamentalmente ha sido diseñada para ser utilizado a nivel empresarial, esta plataforma posee una apariencia acorde a este campo. De todas formas su popularidad en ascenso ha hecho que se convirtiera en uno de los preferidos de los usuarios comunes.

Su enfoque principal apunta hacia la mensajería instantánea, el correo electrónico y otras funciones relacionadas con la comunicación. Es por

ello que los dispositivos de esta marca poseen teclados físicos, pensados y desarrollados para ofrecer facilidad y rapidez para el ingreso de texto.

Otra de las grandes ventajas de esta plataforma reside en su seguridad, lo que ha convertido a los dispositivos BlackBerry en los preferidos de las empresas. .Además posee una arquitectura que trabaja con un verdadero ahorro de energía, lo que permite que con una sola carga el dispositivo funcione mucho más tiempo que los que trabajan con otro software.

Ahora bien, debido a que ha sido pensado para la mensajería, uno de los grandes faltantes de esta plataforma suelen ser las aplicaciones para reproducir archivos multimedia. Además, en general ofrece una escasa oferta de aplicaciones, sobre todo en lo que se refiere a juegos. Cabe destacar que las aplicaciones disponibles suelen tener un costo relativamente elevado.

En cuanto a la personalización, si bien ofrece muchas más alternativas que el iOS, lo cierto es que jamás se lo puede llegar a comparar en este punto con Android.

5. Windows Phone

Windows Mobile, también conocido como Windows Phone, es la versión móvil del sistema operativo de Microsoft, esto por supuesto hace que la plataforma sea compatible con casi todos los programas que funcionan en Windows, entre los que se encuentra la popular suite de oficina Microsoft Office.

Este es uno de los motivos fundamentales por el cual Windows Phone es una de las opciones más elegidas, no sólo por los usuarios comunes, sino también para ser utilizado en el ámbito laboral.

Entre las principales ventajas que reporta la plataforma, además de ser totalmente compatible con todos los productos de Microsoft, cabe mencionar que el diseño de su interfaz gráfica hace posible un usabilidad eficaz.

Por otra parte, si bien no posee soporte para Flash, lo cierto es que ofrece una excelente experiencia de navegación, y tiene una total compatibilidad con HTML5. Otro punto a destacar es sin dudas su desempeño en lo que se refiere a la mensajería instantánea y el correo electrónico. También se destaca la excelente respuesta en el ámbito multimedia y en el mundo de los juegos.

En lo que se refiere a sus desventajas, al tratarse de un sistema de código cerrado no ofrece las posibilidades de customización que brinda Android, siendo más similar en este aspecto a iOS. Además en este caso, las posibilidades de ampliación de sus aplicaciones y demás se encuentran atadas a Zune; la tienda de medios digitales desarrollado por Microsoft que incluye una línea de reproductores multimedia, un servicio de suscripción de música y el reproductor de medios de Windows Phone.

6. Aplicaciones para Smartphones

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

Existen aplicaciones gratuitas o de pago que se descargan por internet directamente al aparato. Suelen ser de fácil instalación y hay infinidad de ellas. A continuación, se mencionan las aplicaciones corporativas más utilizadas:

- **Beluga.** Un servicio de mensajería grupal muy fácil de usar, Beluga, permite que amigos se unan en conversaciones, coordinen actividades y actualicen sus ubicaciones en un mapa, haciendo de és-

ta una app perfecta para organizar reuniones en lugares nuevos.[9] Para iOS y Android.

- **WhatsApp Messenger.** Aplicación de mensajería que permite enviar y recibir mensajes sin pagar por SMS. Usa el plan de datos que se posee, sin generar un costo adicional. Además de aprovechar la mensajería básica, usuarios WhatsApp pueden crear grupos, y enviar entre ellos un número ilimitado de imágenes, videos y mensajes de audio.[10] Disponible para iOS, BlackBerry, Windows Phone y Android.
- **Loopt**. Los usuarios se registran en establecimientos comerciales y pueden publicar preguntas como "¿cuánto cuestan los boletos para el museo?" Otros usuarios que sepan responden en tiempo real. Actualmente Loopt solo cubre grandes ciudades. Para Windows Phone 7.
- **Social Lookout**. Para quienes administran un negocio pequeño, estar al tanto de los temas populares en Facebook, Twitter y Bing o Google News puede ser mucho más valioso que seguir individuos. Se puede consolidar toda esa información en listas usando esta aplicación. Para Windows Phone 7.
- **CrunchSMS**. En CrunchSMS se pueden personalizar los mensajes de texto con fotos, firmas y otros extras interesantes. Hasta puede hacer que los mensajes se vean como burbujas de chat para agregarles algo de diversión. Para BlackBerry.
- **Dropbox**. Es la forma más fácil de sincronizar archivos a través de varios sistemas. Con esta aplicación para dispositivo móvil puede mover archivos rápidamente desde una computadora a un telé-

[9] Consultas en Internet: www.audienciaelectronica.net, (11/10/2013).
[10] Consultas en Internet: www.whatsapp.com, (10/10/2013).

fono sin tener que conectarlo. Para Android, BlackBerry, iOS Apple y Windows Phone 7.

- **Bump.** Permite pasar información fácilmente de un smartphone a otro. Cuando dos dispositivos ejecutando la aplicación se “chocan” físicamente, el contenido seleccionado se transfiere, aún si uno es un iPhone y el otro un dispositivo Android. Para iOS y Android.
- **Gmote**. Con esta app se puede mover el cursor en una PC o Mac usando la pantalla táctil del teléfono. Es la manera perfecta de abrir y cerrar ventanas en la computadora de escritorio o portátil desde el otro lado de la oficina. Para Android.
- **Flipboard.** Permite tener en la pantalla del dispositivo una revista de noticias, fotos, videos y doce redes sociales, novedades de los sitios web favoritos o mensajes recientes de blogs. Para Android.
- **Springpad**. Con Springpad se pueden crear listas de pendientes y establecer recordatorios para aumentar la productividad. Además, se pueden marcar libros, películas u otros artículos que no han sido puestos a la venta para que se recuerde comprarlos después. Para iOS y Android.
- **Taptu**. Es un lector en conjunto de noticias que se ve muy bien y es muy fácil de usar. Se puede escoger qué noticias leer, así como marcar historias interesantes para leerlas después. La aplicación funciona bien aún en áreas con mala recepción. Para iOS y Android.
- **GPS Track Recorder**. Accede al GPS y acelerómetro del celular para determinar la ubicación, velocidad, altitud, distancia y orientación. Pequeñas gráficas muestran la topografía que se ha cubierto. Para Windows Phone 7.

- **Find My iPhone**. Recientemente Apple hizo gratuita esta aplicación para todos los usuarios de iPhone/iPod/iPad. Es la manera más fácil de localizar un dispositivo perdido o robado. Find My iPhone muestra la ubicación aproximada en un mapa. Para iOS Apple.
- **Lookout Mobile Security.** Más que un antivirus para tu teléfono, Lookout permite respaldar el dispositivo en sus servidores y hasta se puede usar para ubicar un teléfono extraviado o hurtado. Lookout mantiene el teléfono a salvo del malware también, escaneando aplicaciones mientras se instalan en el equipo y actualizándose constantemente para poder bloquear nuevas amenazas. Para Android.
- **BlackBerry Protect**. Esta utilidad crea una copia de los datos del teléfono. En caso de pérdida, permite bloquearlo remotamente desde una PC y luego ubicar el dispositivo perdido en un mapa. También se puede hacer que suene a todo volumen si se lo encuentra en la oficina. Para BlackBerry.
- **SuperPassword.** Con esta herramienta de administración de contraseñas, se pueden guardar todas las contraseñas que necesites en el dispositivo móvil con un alto nivel de encriptación para que, si el teléfono desaparece, las posibilidades de que alguien encuentre esa información sean mínimas. Para Windows Phone 7.
- **OfficeSuite Pro 7.** Permite ver, editar, crear, compartir e imprimir documento del paquete Microsoft Office. Incluye un explorador de archivos y se integra con sistemas de almacenamiento en línea como Google Docs y Dropbox. Para Android.
- **Teamviewer.** Permite acceder a datos personales o programas en cualquier lugar, y controlar una PC o Mac fácilmente a distancia

de forma rápida, segura y gratuita. Para Android, Blackberry, iOS y Windows Phone.

- **Skype.** Permite efectuar llamadas gratis, incluso a otros teléfonos. Además, con las últimas versiones se pueden realizar video – llamadas entre contactos, teléfonos, ordenadores e incluso televisores.[11] Para Android, Blackberry, iOS y Windows Phone.
- **AVG Antivirus Gratis.** Antivirus en tiempo real, mejor valorado y gratuito, con protección antirrobo. Protege de virus, *malware*, *spyware* y mensajes de texto nocivos, ayudando a mantener los datos personales a salvo.[12] Para Android, iOS y Windows Phone.

[11] Consultas en Internet: www.skype.com, (15/10/2013).
[12] Consultas en Internet: www.avg.com, (15/10/2013).

CAPÍTULO III

Cómo se transmiten Datos en los Smartphones

Sumario: 1. Red Inalámbrica; 2. Wi-Fi; 3. Bluetooth; 4. GSM; 5. GPRS; 6. Conexión EDGE; 7. Conexión 3G; 8. Conexión 4G.

1.- Red Inalámbrica

Los *Smartphones* tienen la capacidad de transmitir datos mediante las redes inalámbricas.

Tal como su nombre lo indica, las redes inalámbricas son aquellas que carecen de cables. Gracias a las ondas de radio, se lograron redes de computadoras de este tipo, aunque su creación requirió varios años de búsqueda[13].

Esta tecnología facilita en primer lugar el acceso a recursos en lugares donde se imposibilita la utilización de cables, como zonas rurales poco accesibles.

Además, estás redes pueden ampliar una ya existente y facilitar el acceso a usuarios que se encuentran en un lugar remoto, sin la necesidad de

---

[13] Consultas en Internet: www.telcommunity.com/wp-content/uploads/pdf/redes-wireles.pdf, (12/10/2013).

conectar sus computadoras a un *hub* o a un *switch* por intermedio de cables. Estos usuarios podrían acceder a la red de su empresa o a la computadora de su casa en forma inalámbrica, sin configuraciones adicionales.

Muchas veces vamos a escuchar hablar de *wireless*, que es como se le dice a las redes inalámbricas en ingles que su significado es “sin cables”, y se denomina así a los dispositivos que no utilizan cables para realizar el envío, y la recepción de datos.

La principal ventaja que supone una red *Wireless* frente a una de cables, es su movilidad. En la actualidad, muchos usuarios y empleados de empresas requieren para sus tareas acceder en forma remota a sus archivos, trabajos y recursos. La red *Wireless* permite hacerlo sin realizar ninguna tarea compleja de conexión o configuración, y evita que cada usuario viaje hasta su empresa o su casa para poder acceder a los recursos de su red de datos.

En síntesis, la redes inalámbricas (a diferencia de sus antecesoras) son: más simples de instalar, escalables muy fácilmente, menos complejas en su administración.

El hecho de que no posean cables, nos permite adaptarlas a casi cualquier estructura, y prescindir de la instalación de pisos técnicos y la instalación de cables molestos que crucen oficinas, habitaciones familiares y, en algunos casos, hasta baños.

A través de esta tecnología, puede disponerse de conexión a Internet casi en cualquier lugar donde se cuente de tal servicio y, de esta forma, también a todas las ventajas que nos ofrece la Red de redes respecto de la que es comunicación e información.

2.- Wi-Fi

Cuando hablamos de Wi-Fi nos referimos a una de las tecnologías de comunicación inalámbrica mediante ondas más utilizada hoy en día. Wi-Fi, también llamada WLAN (*Wireless* LAN, red inalámbrica) o estándar IEEE 802.11.

En la actualidad podemos encontrarnos con 2 tipos de comunicación Wi-Fi:

- 802.11b, que emite 11 MB/seg.
- 802.11g, más rápida, a 54 MB/seg.

De hecho, con su velocidad y alcance (unos 100-150 metros en hardware asequible) lo convierten en una fórmula perfecta para el acceso a Internet sin cables.

Para tener una red inalámbrica en casa solo necesitaríamos, un punto de acceso, que se conectaría al módem, y un dispositivo Wi-Fi que se conectaría en nuestro aparato. Existen terminales Wi-Fi que se conectan al P.C. por USB, pero son las tarjetas TCI (que se insertan directamente en la placa base) las recomendables, nos permiten ahorrar espacio físico de trabajo y mayor rapidez. Para portátiles podemos encontrar tarjetas PCMI externas, aunque muchos de los aparatos ya se venden con caja integrada.

Con la tecnología Wi-Fi es posible implementar redes que conectan computadoras y otros dispositivos compatibles (Smartphones, consolas de video juegos, impresoras, entre otras) que estén cercanos geográficamente. Estas redes no exigen el uso de cables, ya que efectúan la transmisión de datos a través de radio frecuencia.

Algunas ventajas que ofrece Wi-Fi son:

- Permite al usuario utilizar la red en cualquier punto dentro de los límites de alcance de la transmisión.
- Permite la incorporación rápida de otras computadoras y dispositivos en la red.
- Evita que las paredes sean taladradas o adaptadas para pasar los cables necesarios para conectarse a la banda ancha por ejemplo[14].

La flexibilidad del Wi-Fi es tan grande, que hizo viable la implementación de redes que hacen uso de esta tecnología en muchos lugares, principalmente por las ventajas citadas. De esta forma, es común encontrar redes Wi-Fi disponibles en hoteles, aeropuertos, estaciones de colectivos, bares, restaurantes, centros comerciales, escuelas, universidades, oficinas, hospitales, etc., que ofrecen acceso a Internet, muchas veces de manera gratuita. Para utilizar estas redes, basta con tener una notebook (computadora portátil), un Smartphone o cualquier dispositivo compatible con la tecnología Wi-Fi.

3.- Bluetooth

La tecnología Bluetooth define un estándar de comunicaciones de corto alcance mediante señales de radiofrecuencia que permite la transmisión de datos y voz. La frecuencia radio de operación es la banda ISM de 2.4 GHz, la misma que las redes WLAN 802.11b y 802.11g. Funcionalmente el sistema Bluetooth ha sido diseñado para sustituir los cables a bajo coste. Comparativamente con las redes WLAN el sistema Bluetooth tiene la misma cobertura, menor velocidad, pero un coste de producción mucho menor.

---

[14] Consultas en Internet: www.informatica-hoy.com.ar/aprender_informatica/que_es_wifi.php, (14/10/2013).

WLAN está diseñado como complemento y/o sustituto de las redes de datos cableados. En cambio, Bluetooth está diseñado para la sustitución de los cables de interconexión entre dispositivos[15].

El nombre Bluetooth es un homenaje al rey de Dinamarca y Noruega, Harald Bltand, que en la lengua inglesa es llamado de Harold Bluetooth. El nombre del rey fue escogido por el hecho de haber unificado las tribus de su país, semejantemente a lo que la tecnología pretende hacer: unificar tecnologías diferentes. El símbolo del Bluetooth es la unión de dos runas nórdicas para las letras H y B, sus iniciales[16].

La tecnología es bastante ventajosa, pues permite la comunicación entre diversos dispositivos sin la necesidad de cables. Además de eso, es una tecnología barata. Por esos motivos, el Bluetooth ganó popularidad, haciéndose uno de los principales métodos de conexión entre dispositivos de la actualidad. Entre los dispositivos que pueden ser conectados vía Bluetooth podemos citar: teléfonos celulares, ordenadores, video juegos, impresoras, escaners, mouses, teclados, etc.

La desventaja de esta tecnología es el hecho de su corto alcance. Además de eso, el número máximo de dispositivos conectados al mismo tiempo también es limitado.

Mucha gente cree que el Bluetooth solo existe en los teléfonos móviles, pero el típico símbolo azul de esta tecnología, que permite la transferencia de datos, también es encontrado en muchos otros dispositivos y puede simplificar tu vida de varias maneras.

---

[15] ROIG, Oriol Salent y VALENZUELA GONZALEZ, José Luis, Principios de Comunicaciones Móviles, 1° Edición, Editorial Cúspide, (Cataluña, 2003), pág. 42.

[16] Consultas en Internet: www.informatica-hoy.com.ar/telefonos-celulares/que-es-bluetooth.php, (14/10/2013).

Esta tecnología está presente en teléfonos, computadoras portátiles, sistemas internos de automóviles, auriculares, reproductores de MP3, parlantes, entre muchos otros dispositivos.

Cuando estamos en el trabajo, el Bluetooth se puede utilizar para sincronizar los contactos de la computadora, Smartphone y otros dispositivos portátiles. Esto ayuda a mantener la agenda actualizada y a garantizar el respaldo de los contactos. Para sincronizar, hay que dejar siempre la opción Bluetooth habilitada en los dispositivos deseados, y hay que seguir las instrucciones que cada equipo provee.

Se puede optar por un Mouse y un teclado Bluetooth. Esto puede marcar una gran diferencia a la hora de la limpieza y organización del escritorio y nos va a liberar del largo de los cables.

Por último, los auriculares y micrófonos Bluetooth aumentan la movilidad del usuario y pueden ser extremadamente útiles para usar servicios VOIP (telefonía por Internet).

4.- GSM

El sistema global para las comunicaciones móviles (del inglés *Global System for Mobile Communications*), GSM, y originariamente del francés (*Groupe Spécial Mobile)* es un sistema estándar, libre de regalías, de telefonía móvil digital.

Un cliente GSM puede conectarse a través de su teléfono con su computadora y enviar y recibir mensajes por correo electrónico, faxes, navegar por Internet, acceder con seguridad a la red informática de una compañía (red local/Intranet), así como utilizar otras funciones digitales de transmisión de datos, incluyendo el servicio de mensajes cortos (SMS) o mensajes de textos.

GSM se considera por su velocidad de transmisión y otras características, un estándar de segunda generación (2G). Su extensión a 3G, difiere en su mayor velocidad de transmisión, el uso de una arquitectura de red ligeramente distinta, y sobre todo en el empleo de diferentes protocolos de radio.

5.- GPRS

GPRS es la sigla de *General Packet Radio Services* (servicios generales de paquetes por radio). A menudo se describe como 2.5G, es decir, una tecnología entre la segunda generación (2G) y la tercera generación (3G) de tecnología móvil digital. Se transmite a través de redes de telefonía móvil y envía datos a una velocidad de hasta 114 Kbps. El usuario puede utilizar el teléfono móvil y el ordenador de bolsillo para navegar por Internet, enviar y recibir correo, y descargar datos y soportes. Permite realizar videoconferencias con sus colegas y utilizar mensajes instantáneos para charlar con sus familiares y amigos, esté donde esté. Además, puede emplearse como conexión para el ordenador portátil u otros dispositivos móviles.

GPRS es una evolución de la actual red GSM: no conlleva grandes inversiones y reutiliza parte de las estructuras actuales de GSM. Por este motivo, GPRS tendrá, desde sus inicios, la misma cobertura que la actual red GSM. GPRS es una tecnología que subsana las deficiencias de GSM: velocidad de transferencia de hasta 144 Kbps, conexión permanente, tiempo de establecimiento de conexión inferior al segundo, pago por cantidad de información transmitida, no por tiempo de conexión[17].

El uso de GPRS no se limita solo a los teléfonos móviles. Aparecerán tarjetas PCMCIA GPRS para conectar portátiles a Internet, tarjetas para

---

[17] QUERO CATALINAS, Enrique y GARCIA, Román Agustín, Mantenimiento de Portales de la Información, Editorial Paraninfo, (España, 2007), pág. 10.

conectar el ordenador de sobremesa, etc. El uso de nuevos terminales GPRS con módem inalámbrico tendrá una aplicación inmediata y evidente. Los podremos conectar a ordenadores portátiles o de sobremesa como cualquier módem, pero, evidentemente, con las ventajas de ser inalámbrico.

Igualmente, los terminales GPRS nos permitirán visualizar contenidos y utilizar servicios de Internet directamente en su pantalla reducida, en una evolución continua de convergencia entre el teléfono móvil y los PDA (Asistentes Digitales Personales). La evolución natural de GPRS es UMTS (*Universal Mobile Telephony System*) donde tendremos conferencias en tiempo real.

6.- Conexión EDGE

EDGE es el acrónimo de *Enhanced Data rates for GSM Evolution* (Tasas de Datos Mejoradas para la evolución GSM). También conocida como EGPRS (*Enhanced* GPRS).

Es una tecnología de telefonía móvil celular, que actúa como puente entre las redes 2G y 3G. EDGE se considera una evolución del GPRS. Esta tecnología funciona con redes GSM que tenga implementado GPRS, el operador debe implementar las actualizaciones necesarias, además no todos los teléfonos móviles soportan esta tecnología.

EDGE, o EGPRS, puede ser usada en cualquier transferencia de datos basada en conmutación por paquetes (Packet Switched), como lo es la conexión a Internet. Los beneficios de EDGE sobre GPRS se pueden ver en las aplicaciones que requieren una velocidad de transferencia de datos, o ancho de banda altos, como video u otros servicios multimedia[18].

---

[18] Consultas en Internet: www.es.wikipedia.org/Wiki/Enhanced_Data_Rates_for_GSM_Evolution, (29/08/2013).

Además de usar GSMK (*Gaussian Minimum-Shift Keying*), EDGE usa 8 PSK (8 *Phase Shift Keying*) para los cinco niveles superiores de nueve esquemas totales de modulación y codificación. En los cuatro primeros niveles se utiliza GPRS propiamente dicho. La utilización de 8PSK produce una palabra de 3 bits por cada cambio en la fase de la portadora. Con esto se triplica el ancho de banda disponible que brinda GSM. El nivel del esquema que se utilice para transmitir depende de la relación C/I (portadora/interferente), el cual será más alto cuanto más grande sea el valor C/I. al igual que el GPRS, EDGE usa un algoritmo de adaptación de tasas, que adapta el esquema de modulación y codificación (MCS) usado para la calidad del canal de radio y así el índice binario (*bit rate*) y la robustez de la transmisión de datos. EDGE agrega una nueva tecnología que no se encuentra en GPRS, la ”Redundancia Incremental”, la cual, en vez de re-transmitir los paquetes de información alterados, envía más información redundante que se combina con el receptor, lo cual incrementa la probabilidad de decodificación correcta.

EDGE puede alcanzar una velocidad de transmisión de trescientos ochenta y cuatro Kbps en modo de paquetes, con lo cual cumple con los requisitos de la ITU para una red 3G, también ha sido aceptado por la ITU como parte de IMT-2000, de la familia de estándares 3G. También mejora el modo de circuito de datos llamado HSCSD aumentando el ancho de banda para el servicio.

Aunque la tecnología UMTS es de mayor capacidad de transferencia y cronológicamente más reciente, sus altos costos de implementación y poco apoyo, hace que una buena cantidad de operadores de telefonía móvil celular tengan implementada la tecnología EDGE, dominando el mercado global de las comunicaciones GSM/GPRS.

7.- Conexión 3G

Es la tecnología inalámbrica de tercera generación, el cual es un servicio inalámbrico que permite estar conectado a Internet a través de los teléfonos móviles. Esta tecnología presenta a diferencia de las anteriores una mejor calidad y fiabilidad, una mayor velocidad y ancho de banda superior para aplicaciones más allá de la voz, como audio MP3 y video llamadas. De esta manera se pueden visualizar diferentes contenidos y establecer llamadas con imágenes, facilitando así la introducción de nuevos servicios. Las redes 3G tienen una mayor seguridad a comparación de las tecnologías anteriores. La velocidad que presenta esta tecnología es de hasta 384 kbps, la cual es siete veces más rápida a la de cualquier conexión telefónica estándar[19].

Navegar a alta velocidad sin la utilización de cables ya no es solo una ventaja para quienes poseen teléfonos móviles de alta gama. Actualmente, los operadoras de telefonía celular están vendiendo servicios de Internet banda ancha para quien requiera de un módem compatible con la nueva tecnología.

Además de la alta velocidad, uno de los grandes beneficios que brinda esta tecnología es que permite efectuar video llamadas. Otro recurso que sedujo a los usuarios es la facilidad de acceder a canales de televisión en su móvil[20].

Hay diversas operadoras que tienen disponibles dispositivos compatibles con la tecnología 3G, sin embargo, el equipo más esperado y deseados por muchos es el Iphone 3G. Claro que cada Smartphone tiene sus ventajas, sin embargo, el seductor equipo de Apple lleva la ventaja de

---

[19] Consultas en Internet: www.feederico.com/que-significa-tecnologia-3G-celulares, (29/07/2013).

[20] Consultas en Internet: www.informatica-hoy.com.ar, (13/10/2013).

poseer no solo alta velocidad 3G, sino que también posee atractivos incluidos dentro del aparato, como el sistema *multi-touch*, censor de movimientos, entre otros.

8.- Conexión 4G

En telecomunicaciones, 4G son las siglas utilizadas para referirse a la cuarta generación de tecnologías de telefonía móvil. Es la sucesora de las tecnologías 2G y 3G, y que predice a la próxima generación, la 5G.

La 4G está basada completamente en el protocolo IP, siendo un sistema de sistemas y una red de redes, que se alcanza gracias a la convergencia entre las redes de cables e inalámbricas. Esta tecnología podrá ser usada por módems inalámbricos, *Smartphones* y otros dispositivos móviles. La principal diferencia con las generaciones predecesoras será la capacidad para proveer velocidades mayores de cien MBit/s en movimiento y un Gbit/s en reposo, manteniendo una capacidad de servicio (QoS) de punta a punta de alta seguridad que permitirá ofrecer servicios de cualquier clase en cualquier momento, en cualquier lugar, con el mínimo costo posible.

El concepto 4G va más allá de la telefonía móvil, ya que no puede ser considerada una evolución de los estándares de telefonía celular, tales como las existentes en el mercado actual. Las nuevas tecnologías de redes de banda ancha móvil (inalámbrica) permiten el acceso a datos en dispositivos que operen con IP, desde *handsets* hasta CPEs (equipamiento para conversión de datos para un uso en equipamientos finales tales como televisores y teléfonos)[21].

Los grandes atractivos del 4G es la convergencia de una gran variedad de servicios hasta entonces solamente accesibles con una banda an-

[21] Ibidem.

cha fija, así como la reducción de costos e inversiones para la ampliación del uso de la banda ancha en la sociedad, logrando beneficios culturales, mejoría en la calidad de vida y acceso a servicios básicos tales como comunicación y servicios públicos antes inaccesibles o precarios.

La 4G está siendo desarrollada con el objetivo de ofrecer servicios basados en banda ancha móvil tales *como Multimedia Messaging Service* (MMS), video chat, *Mobile* TV, contenido HDTV, *Digital Video Broadcasting* (DVB), servicios básicos como voz y datos, siempre manteniendo el concepto de uso en cualquier lugar y en cualquier momento. Todos los servicios deberán ser prestados teniendo como premisas el intercambio de paquetes en un ambiente IP, gran capacidad de usuarios simultáneos, banda minima de 100 MBits para usuarios móviles y un GBits para estaciones fijas.

CAPÍTULO IV

Peligros Expuestos en los Smartphones

Sumario: 1. Vulnerabilidad de los sistemas; 2. Vulnerabilidad de Internet y los servicios inalámbricos; 3. Definición y clasificación de los *Hackers*; 4. *Software* malicioso de los *Smartphones*; 5. Peligros latentes de los *Smartphones*.

1.- Vulnerabilidad de los sistemas

Si usara la computadora para manejar el negocio, tal vez no podría vender sus productos a sus clientes o hacer pedidos a sus proveedores mientras estuviera descompuesta. También podría ser que el sistema de información de la computadora hubiera sido penetrado por extraños quienes podrían robar y/o destruir datos valiosos, incluyendo datos de pagos confidenciales de sus clientes. Si se destruyeran o divulgaran muchos datos, quizás su negocio nunca volvería a funcionar.

A medida que aumenta el uso de las tecnologías de la información y la comunicación e Internet, aparecen nuevas amenazas que ponen en riesgo la seguridad de los datos y los sistemas informáticos de las empresas. Éstas han de aprender a enfrentar adecuadamente estos peligros, pues, en caso contrario, las consecuencias pueden llegar a ser realmente graves: pér-

dida de datos, gastos imprevistos, fuertes bajas en la productividad, entre otras.

Un sistema informático seguro reúne varias características principales:

- Integridad: en el sentido en que garantiza la exactitud de la información frente a la alteración, pérdida o destrucción, ya sea de forma accidental o fraudulenta;
- Confidencialidad: es decir, evitar los accesos indebidos a la información y disponibilidad o que los recursos estén disponibles cuando se necesiten[22].

Uno de los activos más importantes que poseen las empresas es la información y, por lo tanto, deben existir técnicas que la aseguren, más allá de la seguridad física que se establezca sobre los equipos en los cuales se almacena. Estás técnicas las brinda la seguridad lógica, que consiste en aplicar barreras y procedimientos que resguarden el acceso a los datos, de manera que solo puedan manejarlos las personas autorizadas y nadie más que ellos.[23]

Si usted opera un negocio en la actualidad, necesita hacer de la seguridad y el control sus principales prioridades. La seguridad se refiere a las políticas, procedimientos y medidas técnicas utilizadas para impedir el acceso no autorizado, la alteración, el robo o el daño físico a los sistemas de información. Los controles consisten en todos los métodos, políticas y procedimientos organizacionales que garantizan la seguridad de los activos más

---

[22] Consultas en Internet: www.riesgossistmeinformatico.blogspot.com.ar, (01/09/2013).

[23] Ibidem.

valiosos de la organización; la precisión y confiabilidad de sus registros contables, el apego de las operaciones a las normas de la administración.

Cuando se almacena en forma electrónica grandes cantidades de datos, son vulnerables a una gran variedad de tipos de amenazas, muchas más que las que existían cuando se almacenaba en forma manual. Los sistemas de información ubicados en diferentes lugares se interconectan por medio de redes de comunicaciones. La posibilidad de acceso no autorizado, abuso o fraude no se limita a una sola ubicación, sino que puede ocurrir en cualquier punto de acceso a la red.

Los *hackers* pueden, valiéndose de una diversidad de artimañas, acceder a los datos que fluyen sobre las redes, robar datos valiosos durante su transmisión o alterar mensajes sin autorización. No está de más aclarar que Internet y otras redes son altamente vulnerables a alteraciones por la radiación. Los intrusos pueden lanzar ataques de negación de servicios o *software* malicioso para alterar el funcionamiento de los sitios Web. Quienes tienen la capacidad de penetrar en los sistemas corporativos pueden destruir o alterar los datos corporativos almacenados en bases de datos o en archivos.

La seguridad informática es importante debido a que sin fuertes medidas de seguridad, los datos valiosos se pueden perder o destruir, o caer en manos equivocadas y revelar secretos comerciales importantes o información que viole la privacidad personal.

2.- Vulnerabilidad de Internet y los servicios Inalámbricos

Las redes públicas grandes, como Internet, son más vulnerables que las internas porque están abiertas a todo el mundo. Internet es tan grande y abierta que cuando ocurren abusos, éstos pueden tener un impacto enormemente generalizado en cuestión de minutos. Cuando las redes corpo-

rativas se enlazan a Internet, los sistemas de información de las empresas son vulnerables a ataques de extraños.

Las modernas redes de banda ancha de alta velocidad no ayudan en este aspecto. Las computadoras conectadas constantemente a Internet por módems de cable o de líneas digitales de suscriptor (DSL) están más abiertas a la intrusión de extraños que las antiguas líneas de marcación telefónica[24].

Los *Hackers* pueden interceptar conversaciones para obtener información de las tarjetas de crédito y de otra información confidencial personal.

La vulnerabilidad se ha incrementado con el uso del correo electrónico y la mensajería instantánea (IM). El correo electrónico podría contener archivos adjuntos que sirven como trampolín para el software malicioso o acceso no autorizado a los sistemas corporativos internos. Los empleados podrían utilizar mensajes de correo electrónico para transmitir secretos comerciales valiosos, datos financieros o información confidencial de clientes a destinatarios no autorizados.

Wi-Fi es una red “abierta” y “no asegurada”. Esto significa que cualquiera puede acceder a ellas, y la comunicación entre su computadora portátil o un teléfono inteligente (*Smartphone*) y el servidor inalámbrico no está encriptada.

Las redes inalámbricas de los hogares tampoco están aseguradas mediante encriptación (aunque ésta es una opción para todas las redes inalámbricas caseras), y los *Hackers* que pasen en automóviles o en bicicleta por las inmediaciones de su casa pueden utilizar fácilmente su red y escuchar sus comunicaciones con un ruteador inalámbrico. Incluso los dispositi-

---

[24] LAUDON, Kenneth C y LAUDON, Jane Price, Sistemas de Información Gerencial,trad. por Antonio Nuñez Ramos, 10° Edición, (Nueva York, s.f.), pág. 317.

vos de comunicaciones Bluetooth tienen evidentes fallas en la seguridad de sus comunicaciones.

Aunque el alcance de las líneas Wi-Fi es de apenas unos metros, puede extenderse hasta poco más de un cuarto de kilómetro utilizando antenas externas; pueden ser fácilmente penetradas por extraños equipados con computadoras portátiles, *Smartphones*, tarjetas inalámbricas, antenas externas y *software* de piratería informática. Los *Hackers* utilizan estas herramientas para detectar redes desprotegidas, monitorear el tráfico de red y, en algunos casos, obtener acceso a Internet o a las redes corporativas.[25]

Las redes inalámbricas de muchos lugares no tienen protecciones básicas contra la "guerra móvil", en la cual los espías conducen cerca de los edificios o se estacionan fuera de ellos e intentan interceptar el tráfico de una red inalámbrica.

3.- Definición y clasificación de los *Hackers*

Un *hacker* es un individuo que intenta obtener acceso no autorizado a un sistema de cómputo. Dentro de la comunidad de la piratería informática, el termino *Cracker* se utiliza comúnmente para denotar a un *Hacker* con intenciones criminales, aunque en la prensa publica, los términos *Hacker* y *Cracker* se emplean de manera indistinta. Los *Hackers* y los *Crackers* obtienen acceso no autorizado encontrando debilidades en las protecciones de seguridad de los sitios Web y los sistemas de cómputo, con frecuencia aprovechando las diversas características de Internet que lo hacen un sistema abierto fácil de utilizar.[26]

---

[25] Ibidem, pág. 318.
[26] Ibidem, pág. 322.

En el mundo de la informática, un *Hacker* es una persona que entra de forma no autorizada a otras computadoras y redes de computadoras. Su motivación varía de acuerdo a su ideología: fines de lucro, como una forma de protesta o simplemente por la satisfacción de lograrlo.[27]

Las actividades de un *Hacker* se han ampliado más allá de la mera intrusión a los sistemas para incluir el robo de bienes o información, así como al daño de los sistemas y al "cibervandalismo", la alteración intencional, destrozo e incluso la destrucción de un sitio Web o un sistema de información corporativo.

Los *Hackers* que intentan ocultar sus verdaderas identidades con frecuencia se falsifican, o distorsionan, a sí mismos mediante direcciones de correo electrónico falsas o haciéndose pasar por otras personas que no son ellos en realidad.

Los *Hackers* han evolucionado de ser grupos clandestinos a ser comunidades con identidad bien definida. De acuerdo a los objetivos que un *Hacker* tiene, y para identificar las ideas con las que comulgan, se clasifican principalmente en: *Hackers* de sombrero negro, *Hackers* de sombrero blanco, *Hackers* de sombrero gris y los *Script Kiddie*.

A continuación vamos a ver en detalle a cada uno de estos tipos de *Hacker* de acuerdo a su clasificación:

- *Hackers* de sombrero negro: se llama *Hacker* de sombrero negro a aquel que penetra la seguridad de los sistemas para obtener una ganancia personal o simplemente por malicia. La clasificación proviene de la identificación de villanos en las películas antiguas del viejo oeste, que usaban típicamente sombreros negros.

---

[27] Consultas en Internet: www.aprenderinternet.about.com/od/conceptos, (01/09/2013).

- *Hackers* de sombrero blanco: Se le llama *Hacker* de sombrero blanco a aquel que penetra la seguridad de los sistemas para encontrar puntos vulnerables. La clasificación proviene de la identificación de héroes en las películas antiguas del viejo oeste, que usaban típicamente sombreros blancos.
- *Hackers* de sombrero gris: Como el nombre sugiere, se le llama *Hacker* de sombrero gris a aquel que es una combinación de sombrero blanco con sombrero negro, dicho en otras palabras: que tiene ética ambigua. Pudiera tratarse de individuos que buscan vulnerabilidades en sistemas y redes, con el fin de luego ofrecer sus servicios para repararlas bajo contrato.
- *Script Kiddie*: Se les denomina *Script Kiddies* a los *Hackers* que utilizan programas escritos por otros para lograr acceder a redes de computadoras, y que tienen muy poco conocimiento sobre lo que está pasando internamente.

La mayor parte de las actividades de un *Hacker*, hoy en día, son delitos penales.

En la actualidad, mientras que los *Hackers* aficionados reconocen los tres tipos de *Hackers* y los *Hackers* de la seguridad informática aceptan todos los usos del término, los *Hackers* del *software* libre consideran la referencia a la intrusión informática como un uso incorrecto de la palabra, y se refieren a los que rompen los sistemas de seguridad como *Crackers* (traducido al español como: “un ladrón de cajas fuertes”).[28]

[28] Consultas en Internet: www.es.wikipedia.org/Wiki/Hacker, (02/09/2013).

4.- ***Software* malicioso de los *Smartphones***

Al *Software* malicioso, o *Malware*, término que surge de las palabras en inglés "*malicious software*", se le considera todo tipo de *software* cuyo objetivo es provocar daños en un sistema informático.

Los programas de *software* malicioso se conocen como *Malware* e incluyen una diversidad de amenazas, como virus de computadora, gusanos y caballos de Troya. Un virus de computadora es un programa de *software* malintencionado al que se adjunta a sí mismo a otros programas de *software* o archivos de datos con el propósito de ejecutarse, por lo general, sin conocimiento o permiso del usuario. La mayoría de los virus de computadora transmiten una "carga útil". Ésta podría ser relativamente benigna, como las instrucciones para desplegar un mensaje o una imagen, o podría ser sumamente destructiva –destruir programas o datos, congestionar la memoria de la computadora, reformatear el disco duro de una computadora u ocasionar que los programas funcionen de manera errática. Por lo general, los virus se esparcen de computadora a computadora cuando los usuarios realizan una acción, como enviar un archivo adjunto en un correo electrónico o copiar un archivo infectado.[29]

Pero además, el concepto de *Malware* es más extenso, ya que se pueden considerar dentro de este tipo de *software* no solo los virus, sino también los gusanos, Troyanos, y otros tipos como veremos en este mismo capítulo más en detalle.

Es necesario diferenciar entre el *Malware*, que siempre es intencionado, con fallos en el *software*, es decir, vulnerabilidades que se suelen conocer como "*Bugs*", o "agujeros de seguridad", que en estos casos no son intencionados, sino que son problemas que se detectan en el *software*, y que

---

[29] LAUDON, Kenneth C y LAUDON, Jane Price, op. cit., pág. 319.

una vez detectados se debe proceder a su corrección lo antes posible para evitar que puedan ser utilizados para atacar al sistema.[30]

Cualquier *software* puede tener "*bugs*", pero es frecuente encontrarlo en un nuevo tipo de *software*, o en las versiones más recientes del mismo, porque en las anteriores ha dado tiempo a que se detecten las vulnerabilidades y se ha podido proceder a la corrección de los "*bugs*" detectados.

Los *Malware* fueron diseñados por expertos en materia de computación y programación con propósitos específicos.

Algunos de los primeros programas infecciosos fueron elaborados como experimentos, como bromas o simplemente como algo molesto, no para causar graves daños en las computadoras. En algunos casos el programador no se daba cuenta de cuánto daño podía hacer a su creación. Algunos jóvenes que estaban aprendiendo sobre los virus los crearon con el único propósito de demostrar que podían hacerlo o simplemente para ver con que velocidad se propagaban. Incluso en 1.999 un virus tan extendido llamado *Melissa* parecía haber sido elaborado tan solo como una travesura.

El software diseñado para causar daños o pérdida de datos suele estar relacionado con actos de vandalismo. Muchos virus son diseñados para destruir archivos en disco duro o para corromper el sistema de archivos escribiendo datos inválidos. Algunos Gusanos son diseñados para vandalizar páginas Web dejando escrito el alias del autor o del grupo por todos los sitios por donde pasan. Estos Gusanos pueden parecer el equivalente informático del *graffiti.*[31]

Sin embargo, debido al aumento de usuarios de Internet, el software malicioso ha llegado a ser diseñado para sacar beneficio de él, ya sea legal o ilegalmente. Desde 2.003, la mayor parte de Virus y Gusanos han sido

---

[30] AGUILERA LOPEZ, Purificación, Seguridad Informática, 11° Edición, Editorial Paraninfo, (España, 2001), pág. 15.

[31] Consultas en Internet: www.es.wikipedia.org/Wiki/Malware, (05/10/2013).

diseñados para tomar control de computadoras para su explotación en el mercado negro. Estas computadoras infectadas son usadas para el envío masivo de *spam* por correo electrónico, para alojar datos ilegales como pornografía infantil, o para unirse en ataques DDoS[32] como forma de extorsión entre otras cosas.

A continuación vamos a clasificar los *Malware* más significativos de entre los muchos tipos de *Software* malicio existentes. Nos vemos a centran en definir únicamente a los Virus, Gusanos, Caballos de Troya y por último, los *Spyware*.

- Virus: El termino Virus informático se usa para designar un programa que, al ejecutarse, se propaga infectando otros software ejecutables dentro de la misma computadora. Los Virus pueden tener también un *pay load* que realice otras acciones a menudo maliciosas, por ejemplo, borrar archivos.
- Gusanos: Un Gusano es un programa que se transmite a sí mismo, explotando vulnerabilidades en una red de computadoras para infectar a otras computadoras. El principal objetivo es infectar a la cantidad posible de usuarios, y también puede contener instrucciones dañinas al igual que los virus. Nótese que un Virus necesita de la intervención de un usuario para propagarse, mientras que un Gusano se propaga automáticamente. Los gusanos y los Virus se propagan a través de Internet desde archivos de software descargado, desde archivos adjuntos a transmisiones de correo electrónicos o desde mensajes comprometidos de correo electrónico o mensajería

[32] Un ataque DDoS o “ataque distribuido de denegación de servicio”, se genera mediante la saturación de los puertos con flujo de información haciendo que el servidor se sobrecargue y no pueda seguir prestando servicios.

instantánea. Hoy en día, también, los Virus y Gusanos se están esparciendo a los dispositivos de comunicación inalámbricos.

- Caballo de Troya: Un Caballo de Troya es un tipo de *software* que aparenta ser benigno pero que hace algo distinto a lo esperado. El Caballo de Troya no es en sí mismo un Virus porque no se replica pero con frecuencia constituye una manera para que los virus y otro código malicioso sean introducidos en un sistema de cómputo. El termino Caballo de Troya se deriva del enorme caballo de madera que utilizaron los griegos para engañar a los troyanos con el fin de que abrieran las puertas de su ciudad fortificada durante la guerra de Troya. Una vez que estuvieron dentro de las murallas de la ciudad, los soldados griegos ocultos en el caballo salieron de éste y capturaron la ciudad.[33]
- *Spyware*: Los programas *Spyware* son creados son creados para recopilar información sobre las actividades realizadas por un usuario y distribuirlas a agencias de publicidad u otras organizaciones interesadas. Algunos de los datos que recogen son las páginas Web que visita el usuario y direcciones de correo electrónico, a las que después se envía *spam* (correo electrónico no deseado). La mayoría de los programas *Spyware* son instalados como Troyanos junto a *software* deseable bajado de Internet. Otros programas *Spyware* recogen la información mediante *cookies* de terceros o barras de herramientas instaladas en navegadores Web. Los autores de *Spyware* que intentan actuar de manera legal se presentan abiertamente como empresas de publicidad e incluyen unos términos de uso, en los que se explica de manera imprecisa el comportamiento del *Spyware*, que los usuarios acepten si leer o sin entender.

---

[33] LAUDON, Kenneth C y LAUDON, Jane Price, op. cit, pág. 321.

Un virus de telefonía móvil es un *software* adaptado a los sistemas operativos de *Smartphones* o dispositivos con capacidad inalámbrica, con el objetivo de perjudicar la funcionalidad del aparato o bien usurpar información de éste.

A medida de que el mercado y consumo de telefonía móvil ha ido creciendo de una manera desorbitada, también ha aumentado la vulnerabilidad de sus sistemas operativos contra ataques informáticos en forma de Virus u otro tipo *software* de tipo *Malware*.

Hasta la fecha se conocen solo dos tipos de Virus para este tipo de dispositivos, clasificados en función de su vía de transmisión a la hora de infectar una terminar:

- Gusano: suelen transmitirse a través de mensajes SMS o MMS, y no requieren interacción del usuario para ser ejecutados. Su principal objetivo es reproducirse y transmitirse a otros aparatos, por lo que pueden copiarse infinitas veces hasta colapsar el propio sistema operativo del terminal e infectar a tantas terminales como disponga a su alcance. También pueden contener instrucciones dañinas.
- Troyano: suele presentarse en formato de archivos ejecutables o aplicaciones descargadas en el dispositivo, aparentemente inofensivas y atractivas al usuario para ser ejecutadas por éste. Al activarse, la parte de *software* malicioso arranca y puede generar numerosos daños, desde la infección e inutilización de otras aplicaciones del propio teléfono dejándolo inutilizable, hasta la usurpación de datos (*Spyware*) sincronizándose con agendas, cuentas de correo, notas y cualquier otra fuente de información para luego ser envia-

dos a un servidor remoto. En este caso, la interacción del usuario es imprescindible para la activación del Virus.

A continuación vamos a describir los Gusanos que afectan a los *Smartphones*:

- Cabir: afecta a los teléfonos móviles que funcionan con el sistema operativo Symbian. Cuando un teléfono está afectado, el mensaje “caribe” se muestra en la pantalla del teléfono y aparece cada vez que éste se enciende. El Gusano intenta propagarse a otras terminales a través de señales inalámbricas *Bluetooth*.
- Commwarrior: conocido como el primer gusano capaz de propagarse entre dispositivos mediante mensajes MMS, tanto por 3G como por *Bluetooth*. Solo afecta a dispositivos que trabajan con el sistema operativo Symbian OS Series 60. Una vez ejecutado el Gusano, éste se propaga mediante la cobertura Bluetooth a otros dispositivos cercanos (un radio aproximado de dieciséis metros) enviados datos infectados con nombres aleatorios.
- Duts: este Virus parasitario infecta archivos y es el primer Virus conocido para la plataforma *Pocket* PC. Intenta infectar todos los archivos ejecutables mayores a cuatro mil noventa y seis *bytes* en el directorio local.
- Skulls: se trata de un fragmento de código Troyano. Una vez descargado, el Virus reemplaza todos los iconos del escritorio del teléfono con imágenes de un cráneo. También inutiliza todas las aplicaciones del teléfono, incluyendo la recepción y envío de SMS y MMS.

- Gingermaster: Troyano desarrollado para plataforma Android que se propaga mediante la instalación de aplicaciones que incorporan de forma oculta el *Malware* para su instalación en segundo plano. Aprovecha la vulnerabilidad de la versión Gingerbread (2.3) del sistema operativo para utilizar los permisos de súper-usuario mediante una escalada de privilegios. Luego crea un servicio que roba información del terminal infectado (identificador del usuario, número SIM, número de teléfono, IMEI, IMSI, resolución de pantalla y hora local) enviando los mismos a un servidor remoto mediante peticiones HTTP.
- DroidKungFu: Troyano contenido en aplicaciones de Android, que al ser ejecutadas, obtiene privilegios de *root* e instala el archivo com.google.ssearch.apk, que contiene una puerta trasera que permite eliminar ficheros, abrir páginas de inicio suministradas, abrir direcciones Web y descargar e instalar paquetes de aplicación. Este Virus recopila y envía a un servidor remoto todos los datos disponibles sobre el terminal.
- Ikee: primer Gusano conocido para la plataforma iOS. Solo actúa en terminales que se les han hecho previamente un proceso de *jailbreak*, y se propaga intentando acceder a otros dispositivos mediante protocolo SSH, primero a través de la subred en la que esté conectado el dispositivo. Luego, repite el proceso generando un rango aleatorio y por último utiliza unos rangos preestablecidos que corresponden a direcciones IP de determinadas compañías telefónicas. Una vez infectado el equipo, sustituye el fondo de pantalla por una fotografía de un cantante famoso.

5.- Peligros latentes en los *Smartphones*

Además de los *Hackers* y del *software* malicioso, los *Smartphones* también se encuentran expuestos a ciertos peligros que pueden ser muy perjudiciales para los usuarios que tengan información importante o confidencial empresarial.

Se mencionan los más relevantes a continuación:

- *Phishing*: En inglés se lee igual que *fishing* (pesca), y es cierto que *Phishing* hace referencia a la pesca, en este caso de contraseñas, de ahí que se haya alterado la palabra *fishing* por una de igual lectura comenzada con P, de *password* (contraseña en inglés). Uno de los aspectos más peligrosos para los usuarios es la estafa electrónica, también denominada *Phishing*, si bien este término inglés se utiliza más específicamente para la obtención fraudulenta de contraseñas.
- *Smishing*: Para muchos usuarios de Internet el ya conocido *Phishing* representa un dolor de cabeza, los *Smartphones* también son blancos de este tipo de ataques, que lo único que pretenden es robar información personal o financiera, por medio por medio de lo que hoy se conoce como *Smishing*[34].

  El Smishing consiste en enviar mensajes de texto falsos, que aparentan venir de entidades de confianza, solicitando que acceda a ciertos enlaces o que se requiere que actualice sus datos de alguna manera. Quienes se dedican a este tipo de delitos informáticos

[34] AGUILERA LOPEZ, Purificación y MORANTE FERNANDEZ, Maria, Informática 4° ESO, Editorial Cúspide, (México, 2008), pág. 114.

mantienen un servidor desde el cual envían mensajes masivos con bases de datos de teléfonos que compran ilegalmente.

- *Spam*: Al envío masivo de correo electrónico basura por parte de terceros, ahora se suman otros canales de comunicación propio de los teléfonos móviles como los mensajes de texto (SMS) y multimedia (MMS) con el fin de distribuir publicidad o en algunos casos propagar códigos maliciosos. Aunque el *Spam* no necesariamente resulta peligroso para la integridad de la información, estadísticas indican que aproximadamente la mitad de los casos están relacionados al fraude, y en los otros representa una molestia o distracción para el usuario.[35]

El correo electrónico basura también puede tener como objetivo a los *Smartphones* a través de mensajes de texto y los sistemas de mensajería instantánea como por ejemplo *Outlook*, *Lotus Notes*, *Windows Live*, etc.

- *Bluetooth*: A todo el mundo le gustan las ventajas de la conexión Bluetooth, la cual permite hablar sin necesidad de sujetar el teléfono a través de dispositivos de manos libres. No obstante, las malas noticias son que el Bluetooth ha sido vulnerable ante posibles amenazas desde que hizo su aparición. El primer *Malware* que atacó este sistema fue el Gusano Cabir, el primer gusano inalámbrico de la historia. Se transmitía teléfonos móviles usando la plataforma Symbian, cuando éstos se encendían y activaban el modo visible. Sin embargo, los efectos no eran realmente dañinos; enviaba un mensaje con un archivo caribe.ss adjunto; una vez que se descargaba el archivo se mostraba la palabra “caribe” en la pantalla. De todos modos, este primer *Malware* fue una llamada de atención al sector.

---

[35] Consultas en Internet: www.eset_la.com, (08/10/2013).

Las amenazas de Bluetooth han evolucionado desde entonces, y aunque siguen sin ser realmente peligrosas se deben tomar en serio.

El *Bluejacking* es, básicamente, *Spam* a través de Bluetooth. A través de esta técnica se envían a usuarios en un radio de diez metros; al descargarse dicha tarjeta, ésta añade el contacto a la agenda ya infectada. Este contacto, además, puede enviar mensajes al dispositivo atacado.

El *Car Wishperer* es un *software* que permite a los atacantes capturar el radio de los coches que dispongan un dispositivo manos libres. Este método permite al atacante escuchar las conversaciones y llamadas que quiera.

Bluebugging es más peligroso que los dos anteriores. Este ataque permite tener acceso remoto al *Smartphone* del usuario y utilizar sus funciones: escucha de llamadas, envío de mensajes, etc. Además, todo esto sucede sin que el dueño del Smartphone se de cuenta. Esto puede suponer una factura mayor de lo habitual, sobretodo, si ha utilizado el *Bluebugging* para realizar llamadas internacionales.

Los ataques a *Bluetooth* explotan las peticiones o procesos de permiso, que son la base de la conectividad *Bluetooth*. A pesar de las funciones de seguridad del *Smartphone*, el único modo de prevenir un ataque de éste tipo es desactivar el *Bluetooth* del dispositivo cuando no se esté usando.

- Redes Sociales: Las redes sociales permiten un nivel de interacción impensado antes de su invención, además han logrado un gran impacto y alcance en poco tiempo. De esta forma, sus características hacen que estos servicios sean muy apetecidos por los usuarios. Sin embargo, lo mismo ocurre con los Ciber criminales o *Ha-*

ckers, quienes invierten tiempo y recursos en crear códigos maliciosos que se propaguen por ésta vía. Por otro lado, una incorrecta configuración de la cuenta de la red social puede exponer información del usuario a terceros, facilitando el robo y suplantación de identidad.

Es recomendable la configuración que ofrecen las redes sociales en estos dispositivos y, si la seguridad no es la óptima, evitar utilizarlas en redes Wi-Fi públicas donde la privacidad de los datos no esté garantizada.

- Tarjeta SIM: Se han descubierto vulnerabilidades de codificación y seguridad en las tarjetas SIM que podrían permitir a terceras personas que tomen el control completo de los teléfonos afectados y espíen las telecomunicaciones de sus víctimas. Se buscó vulnerabilidades en más de mil tarjetas SIM, hasta que se descubrió la forma de explotarlas solo enviando un mensaje de texto oculto y aprovechando una vulnerabilidad en *Java Card*. El mensaje finge provenir del operador de telecomunicaciones del usuario (por ejemplo: Claro, Personal o Movistar) y permite al atacante conseguir la clave de codificación DES de cincuenta y seis *bits* de las tarjetas SIM.

Con ésta información, se puede enviar un mensaje infectado al teléfono comprometido para instalar un Virus que permite espiar al usuario. El programa malicioso le da permiso al atacante para escuchar, redirigir y grabar las llamadas del usuario, robar datos de la Tarjeta SIM, enviar SMS a números *Premium* que cobran al usuario y hasta estafar a los sistemas de pago haciendo compras ilícitas.[36]

[36] Consultas en Internet: www.viruslist.com, (18/10/2013).

CAPÍTULO V

La Seguridad en los Smartphones

Sumario: 1. Seguridad Informática; 2. Seguridad en los Smartphones en entornos corporativos; 3. Software de protección frente al robo y la pérdida; 4. Cifrado o encriptado del dispositivo; 5. Reconocimiento biométrico; 6. Copias de Seguridad; 7. Protección Antivirus; 8. Otras recomendaciones para usuarios.

1. Seguridad Informática

La seguridad informática o seguridad de tecnologías de la información es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. Entre las normas de aplicación, se destacan las que componen las ISO 27000, que se desarrollará en el siguiente capítulo.

La seguridad informática comprende *software* (bases de datos, metadatos, archivos), *hardware* y todo lo que la organización valore (activo) y signifique un riesgo si esta información confidencial llega a manos de otras personas, convirtiéndose, por ejemplo, en información privilegiada.

El concepto de seguridad de la información se diferencia del de "seguridad informática", ya que éste último sólo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos.

Un sistema de información, no obstante las medidas de seguridad que se apliquen, no deja de tener siempre un margen de riesgo.

Para afrontar el establecimiento de un sistema de seguridad es necesario conocer:[37]

- Cuáles son los elementos que componen el sistema. Esta información se obtiene mediante entrevistas con los responsables o directivos de la organización para la que se hace el estudio de riesgos y mediante apreciación directa.
- Cuáles son los peligros que afectan al sistema, accidentales o provocados. Se deduce tanto de los datos aportados por la organización como del estudio directo del sistema mediante la realización de pruebas y muestres sobre el mismo.
- Cuáles son las medidas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos potenciales. Se trata de decidir cuáles serán los servicios y mecanismos de seguridad que reducirían los riesgos al máximo posible.

Tras el estudio de riesgos y la implantación de medidas, debe hacerse un seguimiento periódico, revisando y actualizando las medidas adoptadas.

---

[37] AGUILERA LOPEZ, Purificación, Seguridad Informática, 1° Edición, Editorial Editex S.A., (Madrid, 2010), pág. 9.

Todos los elementos que participan en un sistema de información pueden verse afectados por fallos de seguridad, si bien se suele considerar la información como el factor más vulnerable. El *hardware* y otros elementos físicos se pueden volver a comprar o restaurar, el *software* puede ser reinstalado, pero la información dañada no siempre es recuperable, lo que puede ocasionar daños de diversa índole sobre la economía y la imagen de la organización y, a veces, también causar perjuicios a personas. Otro aspecto a tener en cuenta es que la mayoría de los fallos de seguridad se deben al factor humano.[38]

2. Seguridad en los *Smartphones* en entornos corporativos

Los usuarios de teléfonos móviles inteligentes se han ido incrementando en los últimos años, debido a la extensa variedad de aplicaciones que pueden instalar. La navegación e intercambio de información en internet se ve beneficiada por la mejora de las redes inalámbricas (Wi-Fi), facilitando el envío y recepción de correos electrónicos en cualquier momento, así como la realización de diversas transacciones *online*.

Como bien es sabido, los dispositivos móviles pueden perderse e incluso ser robados. Debido a situaciones como estas debemos asegurarnos de que los datos corporativos estarán siempre seguros y no caerán de ninguna manera en manos equivocadas. Los propios dispositivos poseen diversas posibilidades para apoyar la política de seguridad establecida por la empresa.

Como se mencionó anteriormente, los teléfonos inteligentes tienen varios usos, tanto en un entorno profesional como privado, por lo que garantizar la protección de estas plataformas pasa a ser un reto imprescindible. En

[38] Ibidem.

las empresas, los teléfonos inteligentes se utilizan normalmente para acceder a redes de comunicaciones, principalmente a sistemas de telefonía y de correo electrónico, pero también (y cada vez más) a sistemas de mensajería, incluidos sistemas de gestión y planificación de calendario. También se utilizan para obtener un acceso total a bases de datos de contactos. En estos casos, debe asegurarse la confidencialidad de los datos protegidos de la empresa. No debe permitirse a terceras personas el acceso al correo electrónico empresarial ni, por supuesto, a información de clientes o proveedores.[39]

El paso siguiente implica el acceso a redes corporativas. Los empleados normalmente utilizan una conexión VPN para acceder a la red corporativa desde la que pueden acceder a archivos y aplicaciones empresariales. Es importante que las empresas pasen a la acción en esta etapa para evitar que los usuarios no autorizados accedan a información interna de la empresa, extraigan datos, o manipulen aplicaciones existentes. Durante muchos años, las empresas han implementado estrategias de protección que cubrían los servidores, las estaciones de trabajo y otros recursos de TI. La protección de los teléfonos inteligentes aún no constituye, por desgracia, un componente fijo de las políticas de seguridad corporativas. Debido a los usos indicados anteriormente, proteger los teléfonos inteligentes de la empresa sería un paso muy acertado.

Hay tres situaciones básicas en las que deben protegerse los teléfonos inteligentes[40]:

- pérdida o robo del *Smartphone*

---

[39] KASPERSKY LAB, Los Retos de la Seguridad Móvil en el Entorno Corporativo, Artículo técnico, (Madrid, 2012), pág. 2.

[40] Ibidem, pág. 3.

- situaciones en las que otra persona obtiene acceso completo al dispositivo móvil durante un breve período de tiempo
- todas las demás situaciones de riesgo, incluido el *malware* diseñado específicamente para dispositivos móviles, ataques por SMS y robo de datos concretos mediante correos electrónicos o sitios web desarrollados específicamente para ello.

Para proteger los dispositivos de las situaciones mencionadas, existen distintas consideraciones a tener en cuenta, entre las que se pueden mencionar:

- Utilizar software de protección frente al robo y la pérdida del dispositivo
- Cifrar o encriptar el Smartphone
- Utilizar protección por reconocimiento biométrico, cuando el dispositivo cuente con ello
- Establecer copias de seguridad
- Emplear software de protección antivirus

3. Software de Protección frente al robo y la pérdida

Si pierde o le roban el teléfono inteligente, otra persona puede conseguir acceso físico a su dispositivo. Si quien lo encuentra no es honrado, tiene todo el tiempo del mundo para acceder a la información almacenada en el teléfono. No sólo tienen valor los datos almacenados en el dispositivo móvil, sino que también puede resultar de interés la información de inicio de sesión en redes corporativas o en servicios de telecomunicaciones. Si hay contraseñas de servidores VPN o de correo electrónico almacenadas en el telé-

fono, el ladrón sólo tiene que elegir la aplicación adecuada para obtener acceso a los mismos. [41]

El *software* de protección incluye funciones especiales antirrobo que evitan el acceso de terceras personas a la información de los dispositivos. Los teléfonos que se pierden pueden incluso bloquearse a distancia utilizando un *software* especial de gestión.

Los dispositivos con receptores GPS (una función que ya está incorporada en la mayoría de los teléfonos *smartphones*) también pueden ser localizados fácilmente. También pueden tomarse medidas más drásticas y utilizar un comando de eliminación para restablecer por completo la configuración de fábrica del dispositivo. Aunque siga siendo necesario sustituir el dispositivo perdido, esto no supone un problema para la mayoría de las empresas y restablecer la configuración inicial evita que datos corporativos confidenciales puedan caer en las manos equivocadas.

Un ladrón profesional tomará medidas rápidas para evitar ser detectado. Por tanto, una de sus primeras acciones será retirar la tarjeta SIM. Pero, en ese caso, el *software* de protección cuenta con funciones que permiten localizar el dispositivo aunque se haya retirado la tarjeta SIM. Incluso es posible enviar el número de teléfono de la tarjeta SIM insertada al legítimo dueño del teléfono.

4. Cifrado o Encriptado del dispositivo

La Encriptación de Datos, también conocida como encriptado o cifrado de datos, es un proceso mediante el cual uno o más archivos, documentos, carpetas, o incluso discos completos, son transformados de un for-

---

[41] Ibidem, pág. 4.

mato legible (texto plano o información plana) a un formato ilegible (texto cifrado o información cifrada) para cualquier persona que no posea la llave correspondiente para acceder a dicha información.

En los casos en que el Smartphone no puede ser bloqueado a tiempo, el cifrado resulta muy útil. Este método resultó ser muy eficaz para proteger datos en ordenadores portátiles durante muchos años.

Si se selecciona la función de encriptamiento del teléfono, se establecer un código para poder acceder a los datos y desencriptarlos, que se pedirá cada vez que se encienda el *Smartphone*. Hay que tener bien presente que el proceso de encriptamiento es irreversible. Eso significa que, una vez ejecutado, para echarlo atrás se deberá resetear el dispositivo a sus valores de fábrica, perdiendo así todos los datos alojados en el mismo.

Con el fin de proteger los datos de los usuarios de posibles robos, los proveedores de sistemas operativos móviles han desarrollado diferentes funciones de cifrado. La información importante se guarda en formato cifrado y se descifra cada vez que el usuario introduce su PIN de desbloqueo. Apple no permite a sus usuarios manipular los ajustes de cifrado, pero muchos datos se cifran cuando se activa la función de código de acceso. En los ajustes de seguridad de Android, existe una opción para cifrar el contenido del dispositivo, inhabilitando el acceso a los datos si no se introduce la contraseña. Si no se conociese la clave no sería posible recuperar la información, aunque se utilicen técnicas forenses de extracción y copia de datos. La única forma posible sería con técnicas de fuerza bruta, que consisten en probar automáticamente todas las combinaciones posibles de contraseña, hasta encontrar aquella que permite el acceso. Por tanto, es importante que para que este

ataque sea muy difícil de llevarse a cabo, se utilice una contraseña compleja, que combine letras con dígitos, mayúsculas y caracteres especiales.[42]

5. Reconocimiento biométrico

Existe una forma infalible de contraseña que asegura que sólo el usuario de un dispositivo pueda acceder a él. Hoy en día existen sistemas que permiten la identificación de usuarios por las características únicas de su persona: algo que el usuario es. Esas características representan un patrón propio que no puede coincidir con el de ningún otro individuo, y que además es difícil de reproducir. El estudio de las técnicas de reconocimiento de usuarios utilizando las características corporales propias que lo distinguen de los demás es el objetivo de la Biometría.[43]

La autenticación basada en características físicas existe desde siempre y, sin darnos cuenta, es la que más utiliza cualquiera de nosotros. Todos los días realizamos de forma inconsciente reconocimiento de personas por los rasgos de su cara o por su voz. En el caso de los sistemas biométricos el reconocedor es un dispositivo que, basándose en características del sujeto a identificar, permite o deniega el acceso a un determinado recurso o lugar físico.

La tecnología de los sistemas de identificación biométrica utiliza características fisiológicas que son estables en los individuos. Estas características no se limitan sólo a las huellas dactilares. Existen sistemas basados en reconocimiento de la forma de la mano, de la voz, del iris, de la retina, de la firma, etc.

---

[42] Consultas en Internet: www.blog.kaspersky.es/por-que-debemos-cifrar-nuestros-datos, (30/10/2013)

[43] Consultas en Internet: www.ceditec.etsit.upm.es, (01/10/2013).

Al hablar de los sistemas de este tipo, no estamos hablando de sistemas muy lejanos. Hoy en día existen portátiles y dispositivos móviles que disponen de sistemas de reconocimiento de huella dactilar incorporados, que permiten sustituir los nombres de usuario y contraseñas o bien bloquear el disco duro para mantener la seguridad de los datos.

El uso de la Biometría presenta numerosas ventajas sobre los sistemas de verificación más “tradicionales” basados en contraseñas, a los que además puede complementar. En primer lugar, dado que la propia persona es la portadora de la característica biométrica, no es necesario memorizar ninguna contraseña que se pueda olvidar. Las características biométricas no se pueden perder, y son difíciles de robar, aunque se podría falsificar.

En los *Smartphones*, la autenticación biométrica se realiza utilizando el *hardware* instalado en el terminal móvil, y los datos se almacenan en dicho dispositivo, sin necesidad de recurrir a una base de datos externa centralizada. Los datos biométricos se capturan, procesan y almacenan de forma segura en el propio terminal. La característica biométrica que se podría utilizar depende de varios factores:

- Los sistemas disponibles en el dispositivo móvil
- La capacidad de almacenamiento en memoria
- la capacidad de procesamiento.[44]

6. Copias de seguridad

En determinadas ocasiones un *Smartphone* falla y no se puede hacer nada por solucionarlo. Son situaciones inexplicables que están fuera de

[44] Ibidem.

nuestro alcance y cuya única solución es tener que volver a instalar de nuevo los programas uno por uno. Cuando esto ocurre nos encontramos con que además de haber perdido todas nuestras aplicaciones, también se han borrado nuestros datos, las diferentes configuraciones, los sms, agenda, etc.

Si la información utilizada en el dispositivo es importante, y su pérdida ocasionara graves problemas, entonces sería conveniente utilizar alguna solución de copias de seguridad.

Hay programas que sincronizan los datos almacenados con el ordenador de escritorio, o en alguna aplicación online ofrecida por el fabricante, de forma que los datos están siempre disponibles y actualizados. En caso de pérdida de la terminal, la información seguiría estando disponible y a salvo. Existen algunas aplicaciones que permiten salvaguardar una copia exacta de nuestro sistema. Nuestras aplicaciones, contactos, cuentas de correo y redes sociales configuradas para la sincronización permanecerán en un archivo, creada por la aplicación, esperando a ser restauradas en caso de accidente.[45]

Además de las aplicaciones que se pueden descargar para realizar un *backup*, las compañías de telefonía celular brindan la posibilidad de guardar contactos y archivos importantes cargándolos en la nube. Para este caso, es importante mantener el dispositivo sincronizado con la nube, para ir introduciendo los cambios e ir agregando nuevos archivos que queremos mantener seguros y disponibles en el caso de cambiar de equipo. El tema “nube” se analizará en detalle en el capítulo VII.

Se recomienda que si se utilizan este tipo de opciones, de sincronizar nuestros datos con alguna aplicación online externa a la organización a la que se pertenece, no se sincronice la información confidencial si la hubiera, puesto que dejaría de “estar en sus manos”. Lo recomendable es encontrar

---

[45] Consultas en Internet: www.csirtcv.gva.es, (02/10/2013).

soluciones de copias de seguridad controladas por la organización, para que la información no viaje fuera de ella.[46]

7. Protección Antivirus

Los antivirus son aplicaciones de *software* que han sido diseñados como medida de protección y seguridad para resguardar los datos y aplicaciones de programas maliciosos que tienen el fin de alterar, perturbar o destruir el correcto funcionamiento del *Smartphone*. Se actualizan periódicamente para mantener el equipo siempre protegido y realizan análisis tanto periódicos como en tiempo real.

Los programas de seguridad cuentan con protección contra todo tipo de amenazas. Además de la función antivirus, cuentan con otras prestaciones entre las que se destacan las siguientes:

- Protección contra *malware*
- Protección contra *spyware*
- Protección contra *phishing* y sitios fraudulentos
- Protección en caso de robo. Permite el bloqueo remoto, el borrado de la memoria y avisos cuando se cambia la tarjeta SIM
- Protección frente a transacciones bancarias para que sean seguras
- Servicio de ubicación del dispositivo en caso de extravío
- Administración de aplicaciones
- Análisis en tiempo real de las aplicaciones
- Cortafuegos

---

[46] Ibidem.

- Seguimiento del flujo de datos
- Bloqueo de llamadas y mensajes de texto de números indeseados
- Filtro y bloqueo de mensajes sospechosos
- Gestión de batería y de conexiones de red
- Advertencias de aplicaciones inseguras
- Protección de contactos
- Análisis de archivos adjuntos en los mails recibidos
- Bloqueo de páginas riesgosas
- Reportes vía mail con fotos y ubicación de una persona que intenta desbloquear el teléfono
- Restauración y copias de seguridad
- Detección de intentos de robo de identidad y de datos personales

8. Otras recomendaciones para usuarios

Otras recomendaciones importantes que no se quieren dejar de mencionar, además de las ya expuestas, son las siguientes:

- No almacenar información sensible: La información más delicada de la empresa u organización no debe ser almacenada en los *Smartphones* aunque estén cifrados, puesto que los dispositivos móviles suponen riesgos mayores. Si se ha de acceder a dicha información crítica desde un dispositivo móvil debe hacerse de forma online a servidores seguros.[47]

[47] Ibidem.

- Actualizaciones de *Software*: El *software* del *Smartphone* puede actualizarse para solucionar determinados problemas, actualizar aplicaciones o actualizar la versión empleada del sistema operativo. Ejecutar el software más reciente permite sacar el máximo provecho posible del dispositivo.
- WIFI públicas: Las redes inalámbricas de uso público, o compartido, como las disponibles en hoteles o cafeterías pueden suponer un riesgo. A pesar de que tenga contraseña para poder utilizarse, un atacante podría conectarse y capturar el tráfico de todas las personas que se encuentran conectadas a esa red inalámbrica. Podría entonces analizar el tráfico capturado y recopilar contraseñas o datos confidenciales. Si se va a hacer uso de redes inalámbricas de uso público, se recomienda no acceder a ningún servicio que requiera contraseña, realizar operaciones bancarias o descargar documentos confidenciales.
- Desactivar comunicaciones inalámbricas: Es muy importante desactivar las redes inalámbricas si no se van a utilizar a corto plazo. Las redes más usuales suelen ser WIFI, *Bluetooth*, o infrarrojos. Es posible realizar ataques contra redes inalámbricas, utilizando puntos de acceso falsos, y engañando al dispositivo para que se conecte automáticamente a una red de supuesta confianza. El usuario navegaría entonces sin tener constancia de que el tráfico está siendo monitorizado por un atacante.
- Cargadores públicos: Se han dado casos de fugas de información en dispositivos móviles por haber sido conectados en cargadores públicos. Se debe evitar conectar el dispositivo por USB a cualquier ordenador público, como hoteles o cibercafés, y cualquier otro aparato que no tengamos total confianza en él. Pueden haber sido

manipulados para extraer información de cualquier dispositivo USB al que se conecten.

- Fuentes confiables: Se recomienda instalar sólo las aplicaciones necesarias. Mientras más aplicaciones se instalen, más vulnerabilidades potenciales se agregan al *Smartphone*. Las aplicaciones deben provenir desde fuentes confiables. Entre las opciones de seguridad, los dispositivos poseen configuraciones que sólo permiten instalar y actualizar aplicaciones provenientes de las tiendas oficiales de descargas de la cuenta asociada al equipo. Los atacantes suelen crear aplicaciones maliciosas que parecen legítimas, pero que están diseñadas para infectar el *Smartphone*. Por ello, también es aconsejable instalar aplicaciones que tengan una buena reputación.
- Verificar la lista de permisos de las aplicaciones: Se debe verificar la lista de permisos que solicita cada aplicación. Cada una de las aplicaciones, al momento de ser instaladas, solicita permisos para acceder a determinadas fuentes del dispositivo y a algunos de nuestros datos. Se debe revisar que estos datos sean concordantes con el tipo de aplicación que se desea descargar.

CAPÍTULO VI

Buenas Prácticas para la Seguridad de la Información

Sumario: 1. Origen de la ISO 27000; 2. La Serie 27000; 3. ISO 27002: Buenas Prácticas para la Seguridad de la Información; 4. Gestión de Operaciones y Comunicaciones; 5. Control de Accesos

1. Origen de la ISO 27000

La información es un activo vital para el éxito y la continuidad en el mercado de cualquier organización. El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización.[48]

Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización.

ISO/IEC 27000 es un conjunto de estándares desarrollados por ISO (*International Organization for Standardization*) e IEC (*International Electrotechnical Commission*), que proporcionan un marco de gestión de la seguri-

[48] Consultas en Internet: www.iso27000.es/iso27000.html, (28/09/2013).

dad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.[49]

Desde 1901, y como primera entidad de normalización a nivel mundial, la organización BSI (*British Standards Institution*) es la responsable de la publicación de importantes normas como:

- 1979: Publicación BS 5750 - ahora ISO 9001
- 1992: Publicación BS 7750 - ahora ISO 14001
- 1996: Publicación BS 8800 - ahora OHSAS 18001

La norma BS 7799 de BSI aparece por primera vez en 1995, con objeto de proporcionar a cualquier empresa -británica o no- un conjunto de buenas prácticas para la gestión de la seguridad de su información.

La primera parte de la norma (BS 7799-1) es una guía de buenas prácticas, para la que no se establece un esquema de certificación. Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, la que establece los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente.

Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000.

En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión.

En 2005, con más de 1700 empresas certificadas en BS7799-2, este esquema se publicó por ISO como estándar ISO 27001, al tiempo que se revisó y actualizó ISO17799. Esta última norma se renombra como ISO

---

[49] Ibidem.

27002:2005 el 1 de Julio de 2007, manteniendo el contenido así como el año de publicación formal de la revisión.

En Marzo de 2006, posteriormente a la publicación de la ISO27001:2005, BSI publicó la BS7799-3:2006, centrada en la gestión del riesgo de los sistemas de información.

2. La Serie 27000

A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares.

Hay más de 30 normas de la serie ISO 27000, las cuales están en constante cambio porque la seguridad de la información y las mejores prácticas evolucionan constantemente.

Los rangos de numeración reservados por ISO van de 27000 a 27019 y de 27030 a 27044. Entre las normas que componen la serie, se destacan las siguientes:

- ISO 27000: Publicada el 1 de Mayo de 2009 y revisada con una segunda edición de 01 de Diciembre de 2012. Contiene términos y definiciones que se emplean en toda la serie 27000. La aplicación de cualquier estándar necesita de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión.
- ISO 27001: Publicada el 15 de Octubre de 2005. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones. Sustituye a la BS 7799-2, habiéndose establecido unas condiciones de transición para aquellas empresas certi-

ficadas en esta última. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005 (nueva numeración de ISO 17799:2005 desde el 1 de Julio de 2007), para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.

- ISO 27002: Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO27001 contiene un anexo que resume los controles de ISO 27002:2005.
- ISO 27003: Publicada el 01 de febrero de 2010. No certificable. Consiste en una guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases. Tiene su origen en el anexo B de la norma BS7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.
- ISO 27004: Publicada el 15 de diciembre de 2009. No certificable. Especifica las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados. Estas métricas se usan fundamentalmente para la medición de los componentes de la fase “Do” (Implementar y Utilizar) del ciclo PDCA.

- ISO 27005: Publicada el 4 de Junio de 2008. Establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. El conocimiento de los conceptos, modelos, procesos y términos descritos en la norma ISO/IEC 27001 e ISO/IEC 27002 es importante para un completo entendimiento de la norma ISO/IEC 27005:2008, que es aplicable a todo tipo de organizaciones (por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro) que tienen la intención de gestionar los riesgos que puedan comprometer la organización de la seguridad de la información. Su publicación revisa y retira las normas ISO/IEC TR 13335-3:1998 y ISO/IEC TR 13335-4:2000.
- ISO 27006: Publicada en segunda edición el 1 de diciembre de 2011 (primera edición el 1 de marzo de 2007). Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información. Es una versión revisada de EA-7/03 (Requisitos para la acreditación de entidades que operan certificación/registro de SGSIs) que añade a ISO/IEC 17021 (Requisitos para las entidades de auditoría y certificación de sistemas de gestión) los requisitos específicos relacionados con ISO 27001 y los SGSIs. Es decir, ayuda a interpretar los criterios de acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma
- ISO 27007: Publicada el 14 de Noviembre de 2011. No certificable. Es una guía de auditoría de un SGSI, como complemento a lo especificado en ISO 19011.

- ISO/IEC TR 27008: Publicada el 15 de Octubre de 2011. No certificable. Es una guía de auditoría de los controles seleccionados en el marco de implantación de un SGSI.
- ISO/IEC 27010: Publicada el 20 de Octubre de 2012. Consiste en una guía para la gestión de la seguridad de la información cuando se comparte entre organizaciones o sectores. ISO/IEC 27010:2012 es aplicable a todas las formas de intercambio y difusión de información sensible, tanto pública como privada, a nivel nacional e internacional, dentro de la misma industria o sector de mercado o entre sectores. En particular, puede ser aplicable a los intercambios de información y participación en relación con el suministro, mantenimiento y protección de una organización o de la infraestructura crítica de los estados y naciones.
- ISO 27011: Publicada el 15 de diciembre de 2008. Consiste en una guía de gestión de seguridad de la información específica para telecomunicaciones, elaborada conjuntamente con la ITU (Unión Internacional de Telecomunicaciones).
- ISO/IEC 27013: Publicada el 15 de Octubre de 2012. Es una guía de implementación integrada de ISO/IEC 27001 (gestión de seguridad de la información) y de ISO/IEC 20000-1 (gestión de servicios TI).
- ISO/IEC 27014: En fase de desarrollo, con publicación prevista en 2013. Consistirá en una guía de gobierno corporativo de la seguridad de la información.
- ISO/IEC TR 27015: Publicada el 23 de Noviembre de 2012. Es una guía de SGSI orientada a organizaciones del sector financiero y de seguros y como complemento a ISO/IEC 27002.

- ISO/IEC TR 27016: En fase de desarrollo, con publicación prevista en 2013. Consistirá en una guía de valoración de los aspectos financieros de la seguridad de la información.
- ISO/IEC TS 27017: En fase de desarrollo, con publicación prevista en 2013. Consistirá en una guía de seguridad para *Cloud Computing*.
- ISO/IEC 27018: En fase de desarrollo, con publicación prevista en 2013. Consistirá en un código de buenas prácticas en controles de protección de datos para servicios de computación en *Cloud Computing*.
- ISO/IEC TR 27019: En fase de desarrollo, con publicación prevista en 2013. Consistirá en una guía con referencia a ISO/IEC 27002 para el proceso de control de sistemas específicos al sector de la industria de la energía.
- ISO/IEC 27031: Publicada el 01 de Marzo de 2011. No certificable. Es una guía de apoyo para la adecuación de las tecnologías de información y comunicación (TIC) de una organización para la continuidad del negocio. El documento toma como referencia el estándar BS 25777.
- ISO/IEC 27032: Publicada el 16 de Julio de 2012. Proporciona orientación para la mejora del estado de seguridad cibernética, extrayendo los aspectos únicos de esa actividad y de sus dependencias en otros dominios de seguridad, concretamente: Información de seguridad, seguridad de las redes, seguridad en Internet e información de protección de infraestructuras críticas (CIIP). Cubre las prácticas de seguridad a nivel básico para los interesados en el ciberespacio. Esta norma establece una descripción general de Seguridad Cibernética, una explicación de la relación entre la ciberseguridad y otros tipos de garantías, una definición de las partes interesadas y una descripción de su papel en la seguridad cibernética, una orientación para abordar pro-

blemas comunes de Seguridad Cibernética y un marco que permite a las partes interesadas a que colaboren en la solución de problemas en la ciberseguridad.

- ISO/IEC 27033: Parcialmente desarrollada. Norma dedicada a la seguridad en redes, consistente en 7 partes: 27033-1, conceptos generales (publicada el 15 de Diciembre de 2009 y disponible en iso.org); 27033-2, directrices de diseño e implementación de seguridad en redes (publicada el 27 de Julio de 2012); 27033-3, escenarios de referencia de redes (publicada el 3 de Diciembre de 2010 y disponible en iso.org); 27033-4, aseguramiento de las comunicaciones entre redes mediante *gateways* de seguridad; 27033-5, aseguramiento de comunicaciones mediante VPNs (prevista para 2013); 27033-6, convergencia IP (prevista para 2013); 27033-7, redes inalámbricas (prevista para 2013).
- ISO/IEC 27034: Parcialmente desarrollada. Norma dedicada la seguridad en aplicaciones informáticas, consistente en 5 partes: 27034-1, conceptos generales (publicada el 21 de Noviembre de 2011 y disponible en iso.org); 27034-2, marco normativo de la organización (sin previsión de publicación); 27034-3, proceso de gestión de seguridad en aplicaciones (sin previsión de publicación); 27034-4, validación de la seguridad en aplicaciones (sin previsión de publicación); 27034-5, estructura de datos de protocolos y controles de seguridad de aplicaciones (sin previsión de publicación).
- ISO 27799: Publicada el 12 de Junio de 2008. Es un estándar de gestión de seguridad de la información en el sector sanitario aplicando ISO 17799 (actual ISO 27002). Esta norma, al contrario que las anteriores, no la desarrolla el subcomité JTC1/SC27, sino el comité técnico TC 215.

- ISO 27799:2008 define directrices para apoyar la interpretación y aplicación en la salud informática de la norma ISO / IEC 27002 y es un complemento de esa norma.
- ISO 27799:2008 especifica un conjunto detallado de controles y directrices de buenas prácticas para la gestión de la salud y la seguridad de la información por organizaciones sanitarias y otros custodios de la información sanitaria en base a garantizar un mínimo nivel necesario de seguridad apropiado para la organización y circunstancias que van a mantener la confidencialidad, integridad y disponibilidad de información personal de salud.
- ISO 27799:2008 se aplica a la información en salud en todos sus aspectos y en cualquiera de sus formas, toma la información (palabras y números, grabaciones sonoras, dibujos, vídeos y imágenes médicas), sea cual fuere el medio utilizado para almacenar (de impresión o de escritura en papel o electrónicos de almacenamiento) y sea cual fuere el medio utilizado para transmitirlo (a mano, por fax, por redes informáticas o por correo), ya que la información siempre debe estar adecuadamente protegida.

3 - ISO 27002: Buenas Prácticas para la Seguridad de la Información

La ISO/IEC 27002 proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la información se define en el estándar como "la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos y

completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran)".

La versión de 2005 del estándar incluye las siguientes once secciones principales:

- Política de Seguridad de la Información.
- Organización de la Seguridad de la Información.
- Gestión de Activos de Información.
- Seguridad de los Recursos Humanos.
- Seguridad Física y Ambiental.
- Gestión de las Comunicaciones y Operaciones.
- Control de Accesos.
- Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.
- Gestión de Incidentes en la Seguridad de la Información.
- Gestión de Continuidad del Negocio.
- Cumplimiento.

Dentro de cada sección, se especifican los objetivos de los distintos controles para la seguridad de la información. Para cada uno de los controles se indica asimismo una guía para su implantación. El número total de controles suma ciento treinta y tres entre todas las secciones aunque cada organización debe considerar previamente cuántos serán realmente los aplicables según sus propias necesidades.

Esta norma es una guía de buenas prácticas y no especifica los requisitos necesarios que puedan permitir el establecimiento de un sistema de certificación adecuado.

En septiembre de 2013 se modificó la norma, reduciendo el número de controles de ciento treinta y tres a ciento trece, debido a que se consideró que algunos eran muy específicos o estaban obsoletos.

A finales del último trimestre del año se oficializará el nuevo estándar internacional en “Seguridad de la Información” (ISO 27001:2013), junto con el código de Buenas Prácticas (ISO 27002:2013). Esto dejará a sus predecesores, publicados en 2005, en la obsolescencia.

Entre las secciones mencionadas, las de “Gestión de Operaciones y Comunicaciones” y “Control de Accesos” son de gran relevancia en la implementación de prácticas de seguridad en empresas que se gestionan mediante la utilización de *Smartphones*. Por lo mencionado, se analizarán sus principales puntos de control, objetivos y procedimientos sugeridos.

4. Gestión de Comunicaciones y Operaciones

El dominio “Gestión de las Comunicaciones y las Operaciones” incluye diez objetivos de control:[50]

> **1) Procedimientos Operacionales y responsabilidades:** asegurar la operación correcta y segura de los servicios de procesamiento de información.
>
> Para la gestión y operación de todos los sistemas y servicios de procesamiento de información de la Organización, se deben establecer procedimientos y responsabilidades que incluyan el desarro-

[50] Consultas en Internet: www.blog.segu-info.com.ar/2010/06/dominios-de-iso-27001-e-iso-27002.html, (15/10/2013).

llo de instrucciones adecuadas para la operación y procedimientos de respuesta a incidentes operativos y de información.
Para reducir el riesgo de usos no adecuados, sin intención, por error o negligencia de los sistemas de información se debe implementar, de ser requerido, la segregación de funciones de los diferentes roles establecidos en la organización.

2) Gestión de la Prestación del Servicio por Terceras partes: implementar y mantener un grado adecuado de seguridad de la información y de la prestación del servicio, de conformidad con los acuerdos de prestación del servicio por terceras.
La organización debería verificar la implementación de acuerdos, monitorear el cumplimiento de ellos y gestionar los cambios para asegurar que los servicios que se prestan cumplen los requisitos acordados con los terceros.
Se deben definir normas y controles de seguridad que garanticen la adecuada y eficiente entrega de servicios por parte de proveedores externos. Se deben identificar los posibles riegos de seguridad de la información con relación a los servicios que presta el proveedor externo, para adicionar en el contrato las correspondientes medidas de seguridad que ayudan a la mitigación de estos riesgos.

3) Planificación y Aceptación del Sistema: minimizar el riesgo de fallas en los sistemas.
Los requisitos operativos de los sistemas nuevos se deberían establecer, documentar y probar antes de su aceptación y uso.
Se deben definir los requerimientos sobre la planeación en cuanto a la capacidad que deben tener los sistemas o servicios de procesamiento de la información de la Organización y sobre los controles

que se deben aplicar para la aceptación y desarrollo de actualizaciones o nuevas versiones de los sistemas de información.
Para todas las nuevas actualizaciones a sistemas, nuevas versiones y nuevos sistemas de información se deben establecer criterios de aceptación, se deben realizar planes de pruebas para estos nuevos requerimientos antes de su definitiva aceptación y puesta en producción.

4) Protección contra códigos maliciosos y móviles: proteger la integridad del software y de la información.
El software y los servicios de procesamiento de información son vulnerables a la introducción de códigos maliciosos tales como virus de computador, gusanos en la red, caballos troyanos y bombas lógicas. Los usuarios deberían ser conscientes de los peligros de los códigos maliciosos. Los directores deberían, cuando sea apropiado, introducir controles para evitar, detectar y retirar los códigos maliciosos y controlar los códigos móviles.
Se deben definir los adecuados controles para prevenir y detectar la introducción de código o software malicioso.
Los usuarios y funcionarios de la Organización deben tener conocimiento de los peligros que puede ocasionar el software malicioso o no autorizado. Se deben tomar las precauciones adecuadas para la detección e impedimento de los virus informáticos en los equipos de la Organización.

5) Respaldo: mantener la integridad y disponibilidad de la información y de los servicios de procesamiento de información.
Se deben establecer normas y procedimientos rutinarios que permitan tener respaldo de la información y procesamientos de informa-

ción, realizando copias de seguridad, realizando planes de pruebas y simulaciones de la recuperación oportuna de los datos, registrando eventos o fallos y monitoreo de los equipos.

6) Gestión de la Seguridad de Redes: asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.
La gestión segura de las redes, las cuales pueden sobrepasar las fronteras de la organización, exige la consideración cuidadosa del flujo de datos, las implicaciones legales, el monitoreo y la protección.
También pueden ser necesarios los controles adicionales para proteger la información sensible que pasa por redes públicas.

7) Manejo de los Medios: evitar la divulgación, modificación, retiro o destrucción de activos no autorizada, y la interrupción en las actividades del negocio. Estos medios se deberían controlar y proteger de forma física.
Se deberían establecer procedimientos operativos adecuados para proteger documentos, medios de computador (por ejemplo cintas, discos), datos de entrada, salida y documentación del sistema contra divulgación, modificación, remoción y destrucción no autorizadas.

8) Intercambio de la Información: mantener la seguridad de la información y del software que se intercambian dentro de la organización y con cualquier entidad externa.
Los intercambios de información y de software entre las organizaciones se deberían basar en una política formal de intercambio, eje-

cutar según los acuerdos de intercambio y cumplir la legislación correspondiente.
Se deben establecer acuerdos, procedimientos y normas para el intercambio de información entre organizaciones. Se deben considerar las implicaciones relacionadas con comercio, correo e intercambio electrónico de datos.

9) Servicios de Comercio Electrónico: garantizar la seguridad de los servicios de comercio electrónico y su utilización segura.
Es necesario considerar las implicaciones de seguridad asociadas al uso de servicios de comercio electrónico. Incluyendo las transacciones en línea y los requisitos para los controles. Se deben establecer e implementar controles y normas para proteger el comercio electrónico de amenazas que pueden llevar a actividades fraudulentas, disputas por contratos y divulgación o modificación de la información de la Organización. También se deberían considerar la integridad y disponibilidad de la información publicada electrónicamente a través de sistemas disponibles al público.

10) Monitoreo: detectar actividades de procesamiento de la información no autorizadas.
Se deberían monitorear los sistemas y registrar los eventos de seguridad de la información.
Los registros de operador y la actividad de registro de fallas se deberían utilizar para garantizar la identificación de los problemas del sistema de Información. La organización debe cumplir todos los requisitos legales pertinentes que se aplican a sus actividades de monitoreo y registro. Es recomendable emplear el monitoreo del sis-

tema para verificar la eficacia de los controles adoptados y revisar el cumplimiento de un modelo de política de acceso.

Sintetizando, esto es lo que busca este Dominio: Para los sistemas y servicios de procesamiento de la información e infraestructura de la organización se deben definir y establecer controles que garanticen la seguridad, integridad y disponibilidad de la información.

5. Control de Accesos

El dominio “Control de Accesos” incluye siete objetivos de control:[51]

1) Requisitos del negocio para el control de acceso: controlar el acceso a la información.

El acceso a la Información, a los servicios de procesamiento de información y a los procesos del negocio se debería controlar con base en los requisitos de seguridad y del negocio.

Las reglas para el control del acceso deberían tener en cuenta las políticas de distribución y autorización de la información.

2) Gestión del acceso de usuarios: asegurar el acceso de usuarios autorizados y evitar el acceso de usuarios no autorizados a los sistemas de información.

Se deberían establecer procedimientos formales para controlar la asignación de los derechos de acceso a los sistemas y servicios de información.

Los procedimientos deberían comprender todas las fases del ciclo

[51] Ibidem.

de vida del acceso del usuario, desde el registro inicial de los usuarios nuevos hasta la cancelación final del registro de usuarios que ya no requieren acceso a los servicios y sistemas de información. Se debería poner atención especial, según el caso, a la necesidad de controlar la asignación de derechos de acceso privilegiado que permiten a los usuarios anular los controles del sistema.

3) Responsabilidades de los usuarios: evitar el acceso de usuarios no autorizados, el robo o la puesta en peligro de la información y de los servicios de procesamiento de Información.

La cooperación de los usuarios autorizados es esencial para la eficacia de la seguridad.

Se deberla concientizar a los usuarios sobre sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular con relación al uso de contraseñas y a la seguridad del equipo del usuario.

Es recomendable implementar una política de escritorio y pantalla despejados para reducir el riesgo de acceso no autorizado o daño de reportes, medios y servicios de procesamiento de Información.

4) Control de Acceso a las Redes: evitar el acceso no autorizado a los servicios en red.

Es recomendable controlar el acceso a los servicios en red, tanto internos como externos.

El acceso de los usuarios a las redes y a los servicios de red no debería comprometer la seguridad de los servicios de red garantizando que:

- Existen interfases apropiadas entre la red de la organización y las redes que pertenecen a otras organizaciones. y las redes públicas:
- Se aplican mecanismos adecuados de autenticación para los usuarios y los equipos.
- Se exige control de acceso de los usuarios a los servicios de información.

5) Control de Acceso al Sistema Operativo: evitar el acceso no autorizado a los sistemas operativos.

Se recomienda utilizar medios de seguridad para restringir el acceso de usuarios no autorizados a los sistemas operativos. Tales medios deberían tener la capacidad para:

- autenticar usuarios autorizados, de acuerdo con una política definida de control de acceso;
- registrar intentos exitosos y fallidos de autenticación del sistema;
- registrar el uso de privilegios especiales del sistema;
- emitir alarmas cuando se violan las políticas de seguridad del sistema;
- suministrar medios adecuados para la autenticación:
- cuando sea apropiado, restringir el tiempo de conexión de los usuarios.

6) Control de Acceso a las aplicaciones y a la información: evitar el acceso no autorizado a la información contenida en los sistemas de aplicación

Se deberían usar medios de seguridad para restringir el acceso a los sistemas de aplicación y dentro de ellos.
El acceso lógico al software de aplicación y a la información se debería restringir a usuarios autorizados.
Los sistemas de aplicación deberían:

- controlar el acceso de usuarios a la información y a las funciones del sistema de aplicación, de acuerdo con una política definida de control de acceso;
- suministrar protección contra acceso no autorizado por una utilidad, el software del sistema operativo y software malicioso que pueda anular o desviar los controles del sistema o de la aplicación:
- no poner en peligro otros sistemas con los que se comparten los recursos de información

7) Computación Móvil y Trabajo Remoto: garantizar la seguridad de la información cuando se utilizan dispositivos de computación móviles y de trabajo remoto.
La protección necesaria debería estar acorde con los riesgos que originan estas· formas específicas de trabajo. Cuando se usa la computación móvil, se deberían tener en cuenta los riesgos de trabajar en un entorno sin protección y aplicar la protección adecuada.
En el caso del trabajo remoto, la organización debería aplicar protección en el sitio del trabajo remoto y garantizar que se han establecido las disposiciones adecuadas para esta forma de trabajo.

Requisitos de la Norma con este Dominio:[52]

1) Administración de Accesos de usuarios: Se debe definir, establecer, documentar y revisar mensualmente la política de control de acceso con base en los requisitos del negocio de la Organización y de la seguridad para el acceso a los activos y sistemas de información. En esta política deben establecerse las reglas y derechos de cada usuario o grupo de usuarios.

Todos los usuarios y proveedores de servicios de la Organización deben estar informados de los controles que deben seguir, según la política de control de acceso establecida, a los diferentes sistemas de información y activos con los que interactúan en la Organización.

Se deben establecer procedimientos para controlar la asignación de los derechos de acceso a los sistemas y servicios de la Organización, los cuales deben abarcar las etapas del ciclo de vida del acceso de los usuarios, desde el registro inicial de nuevos usuarios hasta su eliminación o desactivación cuando ya no sea requerido dicho acceso a los sistemas de información y servicios de la Organización.

Para los usuarios que tengan acciones privilegiadas en los sistemas y servicios de información, se deben definir y establecer derechos con acceso privilegiado que permita a estos usuarios evitar controles del sistema o ingresar a información y servicios de administración de más alto perfil.

---

[52] Ibidem.

• Registro de usuarios: Para el registro y cancelación de usuarios para acceder a los diferentes sistemas y servicios de información multiusuarios de la Organización debe definirse y establecerse un procedimiento de registro y desactivación de usuarios, el cual debe incluir:

- Identificador único para cada usuario.
- Comprobación de la autorización del usuario por el propietario del servicio para utilizar el sistema o servicio de información.
- Verificación del nivel ce acceso asignado.
- Entrega a usuario de relación escrita de sus derechos de acceso.
- Mantenimiento de un registro formalizado.
- Eliminación inmediata de autorizaciones de acceso a usuarios que dejan la organización.

• Administración de privilegios: La asignación y uso de privilegios en controles de acceso a los sistemas y servicios de información de la Organización deben estar restringidos y controlados.

• Administración de contraseñas para usuario: La asignación de contraseñas debe estar controlada mediante un proceso de gestión formal.

Las contraseñas deben estar almacenadas en un sistema informático protegido mediante tecnologías diferentes a las utilizadas para la identificación y autenticación de usuarios.

- Revisión de los derechos de acceso de los usuarios: Se debe establecer un proceso formal de revisión mensual de los derechos de acceso de los usuarios, para mantener un control efectivo del acceso a datos y servicios de información de la organización.

2) Responsabilidades de los usuarios: Los empleados de la Organización deben estar conscientes de las responsabilidades que tiene a cada uno con relación al mantenimiento de la eficacia de las medidas de control de acceso a los sistemas y servicios de información de la Organización. Cada usuario debe tener en cuenta las buenas prácticas de seguridad de selección y uso de sus contraseñas.

Los usuarios y proveedores de servicio de la Organización deben garantizar que los equipos informáticos desatendidos estén debidamente protegidos. Para esto deben tener conocimiento de los requisitos de seguridad y de los procedimientos para la protección de los equipos desatendidos, así como de las responsabilidades que ellos tienen asignadas para la implementación de dicha protección.

El usuario es orientado en este aspecto y existen consecuencias definidas por incumplimiento que entran aplicarse en el momento de la investigación del incidente presentado.

Se debe adoptar una política de escritorio despejado para reportes y medios de almacenamiento removibles y política de pantalla despejada para los servicios de procesamiento de información.

3) Control del Acceso de los Usuarios a red corporativa: El administrador del centro de cómputo principal de la Organización debe

asegurar que los accesos a las redes y sus servicios no comprometan la seguridad de la infraestructura ubicada en esa locación y los aspectos relacionados con ella.

Los usuarios de la Organización únicamente deben tener permiso de acceso directo a las aplicaciones y bases de datos, para cuyo uso están específicamente autorizados. Este control es importante aplicarlo en conexiones a aplicaciones sensible, críticas o utilizadas por usuarios que se encuentren conectados desde lugares de alto riesgo.

Todos los accesos de los usuarios remotos a sistemas y aplicaciones de información de la Organización deben estar controlados por medio de autenticación.

Se debe seleccionar un método de autenticación que será utilizado por la Organización, por medio de una evaluación de riesgos para determinar el nivel de protección que se requiera.

Todas las conexiones remotas que se realicen a sistemas de información de la Organización deben ser autenticadas. Un medio para autenticar conexiones de equipos y ubicaciones específicas es la identificación automática de los equipos a la red.

Los puertos empleados para diagnóstico remoto y configuración deben estar controlados de forma segura, deben estar protegidos a través de un mecanismo de seguridad adecuado y un procedimiento para asegurar que los accesos lógicos y físicos a estos son autorizados por el director del servicio informático y el personal de mantenimiento de hardware y software que solicita el acceso.

En las redes de la Organización se deben separar los grupos de servicios de información, usuarios y sistemas de información, para evitar accesos no autorizados a los sistemas actuales de información que se encuentran conectados a las redes. Los criterios que se

utilicen para realizar la separación de las redes en dominios debe tener en cuenta la política de control de accesos.

Se debe restringir la capacidad de los usuarios y aplicar controles para conectarse a la red dentro de las redes compartidas de la Organización según la política de control de acceso.

Se deben aplicar controles de enrutamiento para el aseguramiento de las conexiones entre computadores y flujos de información para asegurar que no se incumpla la política de control de acceso a las aplicaciones.

Cada uno de los usuarios de la Organización es responsable de usar de forma adecuada los recursos de red y de seguir los procedimientos definidos para acceder a cada uno de los que tenga disponibles para realizar sus labores.

4) Control de acceso al sistema operativo: Todo acceso a los sistemas operativos de la Organización debe estar controlado por registros de inicio seguro. Es importante tener en cuenta la identificación automática de terminales para la autenticación de conexiones a sitios específicos y a equipos portátiles. Se debe definir un procedimiento para la conexión de los usuarios al sistema informático el cual minimice la posibilidad de accesos no autorizados.

Los procesos de conexión empleados deben mostrar el mínimo de información posible sobre el sistema, para no facilitar ayuda innecesaria a usuarios no autorizados. Los mecanismos seguros de "login" se encuentran documentados en los manuales de usuario de las diferentes aplicaciones.

Se debe limitar y mantener controlado el uso de programas utilitarios del sistema, los cuales sean capaces de eludir medidas de control del sistema o de las aplicaciones. Para las terminales utilizadas

por la Organización se debe definir un período de tiempo de inactividad.

Las terminales inactivas en sitios de alto riesgo, en áreas públicas o no cubiertas por el sistema de seguridad de la Organización deben ser desactivadas después de que se cumpla el periodo de tiempo de inactividad previamente definido, para impedir el acceso a estas por usuarios no autorizados.

El dispositivo que realiza la desactivación debe borrar la pantalla y cerrar las aplicaciones y sesiones de conexión a red después de cumplido el periodo de inactividad. Para reducir accesos no autorizados a terminales que manejan aplicaciones de alto riesgo, se deben implementar restricciones en los tiempos de conexión, se debe limitar el periodo de tiempo en el cual se aceptan conexiones desde una terminal.

5) Control de acceso a las aplicaciones: El acceso lógico al software, a la información y a las funciones del sistema de aplicación de la Organización debe estar restringido únicamente para usuarios autorizados, de acuerdo con la política de control de acceso definida. Se deben definir controles de acceso únicamente para los usuarios propietarios de la información, incluso a personal autorizado o a grupos específicos de usuarios.

Se deben identificar los sistemas sensibles de la Organización para darles un tratamiento especial, por lo tanto éstos deben tener un entorno informático dedicado o aislado.

6) Seguridad En Computación Móvil Y Teletrabajo: Se debe aplicar la protección adecuada y se deben considerar los riesgos de

trabajar en un entorno desprotegido cuando se utiliza la computación móvil.

Se debe implementar la protección requerida en el lugar de trabajo remoto y asegurar que existen acuerdos adecuados para estos tipos de trabajo.

- **Computación Móvil:** Cuando se requiera en la Organización de la utilización de dispositivos de computación móvil, como portátiles, agendas, calculadoras y teléfonos móviles, se debe asegurar que la información no se vea comprometida, se debe establecer una política que tenga presente los riesgos de trabajar con dispositivos de computación y comunicaciones móviles, especialmente en entornos desprotegidos.

  En lugares públicos o áreas desprotegidas que estén fuera del alcance de seguridad de la organización, se debe tener especial cuidado cuando se utilicen dispositivos móviles, se deben instalar en estos dispositivos una protección adecuada para evitar el acceso no autorizado a la divulgación de la información almacenada y procesada por éstos.

  Los dispositivos de computación móvil deben estar protegidos físicamente contra robo.

- **Trabajo remoto:** Cuando se requiera trabajar de manera remota para la Organización, es decir, fuera de las instalaciones de la organización, se debe proteger adecuadamente el lugar de trabajo remoto contra: robo del equipo o información, distribución no autorizada de información de la Organización, accesos remotos no autorizados a los sistemas internos o mal uso de dispositivos. Se deben implementar controles y planes

operativos para las actividades de trabajo remoto sobre el centro de cómputo principal de la Organización. Se deben tener en cuenta los siguientes controles:

- Aprovisionamiento del equipo o mobiliario adecuados para las actividades de trabajo remoto.
- Definición del trabajo permitido, horas de trabajo, clasificación de la información que puede ser utilizada y sistemas y servicios internos.
- Suministro de equipo de comunicación adecuado.
- Seguridad física.
- Proporcionar soporte y mantenimiento para hardware y software.
- Auditoría y seguimiento de respaldo.

CAPÍTULO VII
Cloud Computing

Sumario: 1. Origen del Cloud Computing; 2. Concepto de Cloud Computing; 3. Características del Cloud Computing; 4. Ventajas del Cloud Computing; 5. Desventajas y Riesgos del Cloud Computing; 6. Seguridad y Privacidad de los Datos.

1. Origen del *Cloud Computing*

En las últimas décadas los procesos de deslocalización e internacionalización de las grandes empresas, unidos a la explosión en el uso la de tecnologías de información y procesamiento de datos, han hecho que las necesidades de cómputo de las grandes empresas y organizaciones hayan crecido a un ritmo superior al que lo hacía la capacidad de cálculo de los ordenadores personales. Por este motivo, y para satisfacer las necesidades de los sistemas de computación más exigentes, se ha producido una interesante evolución de las arquitecturas de cálculo, basada fundamentalmente en la ejecución simultánea de procesos en múltiples equipos informáticos. Esta tendencia fue impulsada originalmente por la utilización de sistemas abiertos,

interoperables y protocolos de comunicación estándar que permitían la comunicación eficiente entre sistemas y tecnologías heterogéneos. [53]

El primer paso de esta evolución fue en gran medida propiciado por los sistemas operativos que permitieron la configuración de *clusters*, es decir, agrupaciones de ordenadores con componentes de hardware comunes que se comportan como un único computador.

Tras varias décadas de investigaciones y desarrollos en estas tecnologías, la irrupción del sistema operativo Linux y sus estándares abiertos permitió implementar *clusters* basados en la arquitectura estándar de los PC, consiguiendo instalaciones de cálculo de alto rendimiento a bajos precios y popularizando esta solución durante la década de 1990.

Estos *clusters* sufrieron un proceso de especialización para proporcionar servicios de cálculo y almacenamiento, fundamentalmente en centros de investigación y universidades. Estos centros comenzaron a ofrecer sus servicios a terceros a través de protocolos estándar, constituyendo la denominada arquitectura de computación *grid*, orientada al procesamiento en paralelo o al almacenamiento de gran cantidad de información.

Estas arquitecturas fueron acogidas en instituciones investigadoras durante la primera mitad de la década de 2000, pero la complejidad para utilizar la infraestructura, las dificultades para utilizar diferentes *grids*, y los problemas de portabilidad entre ellas, hicieron que nunca se popularizara fuera del ámbito de la investigación y académico.

Durante esta misma época comenzaron a popularizarse las tecnologías de virtualización que hacían posible implementar máquinas virtuales que desacoplan el *hardware* del *software* y permiten replicar el entorno del usuario sin tener que instalar y configurar todo el software que requiere cada

---

[53] URUEÑA, Alberto, El Estudio Cloud Computing. Retos y Oportunidades, (España, Mayo de 2012), pág. 12.

aplicación. Esto tiene ventajas en la distribución y mantenimiento de sistemas de *software* complejos y permite integrar bajo un mismo entorno un conjunto de sistemas heterogéneos.

Esta nueva arquitectura permitía distribuir carga de trabajo de forma sencilla, lo cual elimina los problemas que presentaba la arquitectura grid, abriendo una nueva puerta al cálculo distribuido, llamado *Cloud Computing*. Este nuevo modelo emerge como un nuevo paradigma capaz de proporcionar recursos de cálculo y de almacenamiento que, además, resulta especialmente apto para la explotación comercial de las grandes capacidades de cómputo de proveedores de servicios en Internet.[54]

2. Concepto de *Cloud Computing*

La revolución tecnológica que actualmente estamos viviendo bien podría ser la más profunda de nuestra historia. Los servicios convergen y pasan del mundo físico al mundo digital, siendo accesibles desde cualquier dispositivo. Un hecho relevante es que los datos ya no residen en los ordenadores sino en una Internet Global que adquiere entidad propia y se convierte en mucho más que una simple infraestructura de conexión: es la plataforma que ofrece servicios a millones de dispositivos inteligentes conectados a la red. Es lo que se conoce como *Cloud Computing* o Informática en la Nube de internet, que permite que los consumidores, empresas o particulares, no se tengan que preocupar de cómo se provee en servicio que necesitan.

Este nuevo concepto de computación comenzó a utilizarse en el 2006 por determinados proveedores de Internet como Google, Amazon, Microsoft y otros más que habían conseguido construir en sus organizaciones un sistema de recursos distribuidos de manera horizontal, introducidos como

---

[54] Ibidem, pág. 13.

servicios virtuales de TI, escalados masivamente y manejados como recursos configurados y mancomunados de manera continua.[55]

Atendiendo a la definición dada por el NIST (*National Institute of Standards and Technology*), el *Cloud Computing* es un modelo tecnológico que permite el acceso ubicuo, adaptado y bajo demanda en red a un conjunto compartido de recursos de computación configurables compartidos (por ejemplo: redes, servidores, equipos de almacenamiento, aplicaciones y servicios), que pueden ser rápidamente aprovisionados y liberados con un esfuerzo de gestión reducido o interacción mínima con el proveedor del servicio.

Otra definición complementaria es la aportada por el RAD Lab de la Universidad de Berkeley, desde donde se explica que el *Cloud Computing* se refiere tanto a las aplicaciones entregadas como servicio a través de Internet, como el *hardware* y el *software* de los centros de datos que proporcionan estos servicios. Los servicios anteriores han sido conocidos durante mucho tiempo como *Software as a Service* (SaaS), mientras que el *hardware* y *software* del centro de datos es a lo que se llama nube.

Se entiende que el *Cloud Computing* representa un cambio importante en cómo pueden las empresas y Organismos Públicos procesar la información y gestionar las áreas TIC; apreciándose que con la gestión TIC tradicional las empresas realizan cuantiosas inversiones en recursos, incluyendo *hardware*, *software*, centros de procesamiento de datos, redes, personal, seguridad, etc.; mientras que con los modelos de soluciones en la nube se elimina la necesidad de grandes inversiones y costes fijos, transformando

---

[55] DE PABLOS HEREDERO, Carmen, LÓPEZ HERMOSO, José Joaquín, ROMO ROMERO, Santiago Martín, MEDINA SALGADO, Sonia, Organización y transformación de los Sistemas de Información en la Empresa, (Madrid, 2011), pág. 128.

a los proveedores en empresas de servicios que ofrecen de forma flexible e instantánea la capacidad de computación bajo demanda.[56]

Como principales agentes intervinientes en el negocio se pueden definir los siguientes:[57]

- **Proveedor:** El proveedor presta servicios a través de la nube a suscriptores o intermediarios, es decir, el servicio ofertado por la empresa proveedora al cliente, ya sea de forma directa o a través de un intermediario.
- **Intermediario:** El intermediario presta servicios de intermediación entre los usuarios finales y los proveedores en un mercado dinámico de oferta y demanda como es el *Cloud Computing*. Como ejemplo se pueden mencionar los servicios frontales o las intermediaciones extremo-extremo.
- **Habilitador:** Se trata de un agente proveedor típicamente enfocado al mercado de proveedores de *Cloud*. Son empresas que proveen de *software* y *hardware* a proveedores de servicios *Cloud*, para que éstos desarrollen y ofrezcan al usuario servicios en la nube.
- **Auditor:** El auditores el agente encargado de llevar a cabo las evaluaciones independientes de los servicios en la nube, de las operaciones asociadas a los sistemas de información, del rendimiento y de la seguridad en el uso de la solución *Cloud*.
- **Suscriptor:** La figura denominada suscriptor se corresponde con el usuario contratante de los servicios *Cloud*, por lo que se puede

---

[56] CIERCO, David, Cloud Computing: Retos y Oportunidades, (Madrid, febrero de 2011), pág. 5.

[57] URUEÑA, Alberto, op. cit., pág. 22.

identificar a esta figura como el cliente de los proveedores, los intermediarios y los auditores.

3. Características del *Cloud Computing*

Entre las características asociadas al *Cloud Computing* se encuentran las siguientes:

- **Pago por uso:** Una de las características principales de las soluciones *Cloud* es el modelo de facturación basado en el consumo, es decir, el pago que debe abonar el cliente varía en función del uso que se realiza del servicio *Cloud* contratado.
- **Abstracción:** Característica o capacidad de aislar los recursos informáticos contratados al proveedor de servicios *Cloud* de los equipos informáticos del cliente. Esto se consigue gracias a la virtualización, con lo que la organización usuaria no requiere de personal dedicado al mantenimiento de la infraestructura, actualización de sistemas, pruebas y demás tareas asociadas que quedan del lado del servicio contratado.
- **Agilidad en la escalabilidad:** Característica o capacidad consistente en aumentar o disminuir las funcionalidades ofrecidas al cliente, en función de sus necesidades puntuales sin necesidad de nuevos contratos ni penalizaciones. De la misma manera, el coste del servicio asociado se modifica también en función de las necesidades puntuales de uso de la solución. Esta característica, relacionada con el pago por uso‖, evita los riesgos inherentes de un posible mal dimensionamiento inicial en el consumo o en la necesidad de recursos.

- **Multiusuario:** Capacidad que otorga el *Cloud* que permite a varios usuarios compartir los medios y recursos informáticos, permitiendo la optimización de su uso.
- **Autoservicio bajo demanda:** Esta característica permite al usuario acceder de manera flexible a las capacidades de computación en la nube de forma automática a medida que las vaya requiriendo, sin necesidad de una interacción humana con su proveedor o proveedores de servicios *Cloud*.[58]
- **Acceso sin restricciones:** Característica consistente en la posibilidad ofrecida a los usuarios de acceder a los servicios contratados de *Cloud Computing* en cualquier lugar, en cualquier momento y con cualquier dispositivo que disponga de conexión a redes de servicio IP. El acceso a los servicios de *Cloud Computing* se realiza a través de la red, lo que facilita que distintos dispositivos, tales como teléfonos móviles, tabletas u ordenadores portátiles, puedan acceder a un mismo servicio ofrecido en la red mediante mecanismos de acceso comunes.

Las soluciones de *Cloud Computing* se clasifican como sigue:

- ***Cloud* Público (Externo):** Forma de implementación caracterizada por la oferta de servicios de computación virtualizados (bases de datos, sistemas operativos, plataformas de desarrollo, aplicaciones, etc.) por parte de los proveedores para múltiples clientes, accediendo éstos a dichos servicios a través de Internet o redes privadas virtuales (VPNs).

---

[58] CIERCO, David, op. cit., pág. 36.

Como características inherentes a esta forma de implementación podemos citar las que siguen:

- Reducido plazo de tiempo para la disponibilidad del servicio.
- No se requiere llevar a cabo inversión monetaria para su implementación.
- Permite la externalización a un proveedor de servicios cloud de todas las funciones básicas de la empresa.
- Posibilita el aprovechamiento de la infraestructura de los proveedores de servicios, permitiendo adicionalmente una alta escalabilidad y flexibilidad en la modificación del dimensionamiento del servicio.
- Favorece la utilización de conjuntos de software estándar.
- Lleva asociadas unas cuotas iniciales de pago más bajas que el resto de implementaciones. Adicionalmente los costes del *Cloud* público son variables, cumpliendo el principio de pago por uso.
- La información corporativa se encuentra alojada en la nube pública junto a la del resto de clientes del proveedor, lo que implica, además de no poder tener localizada físicamente dicha información, imponer al proveedor una serie de requisitos de alta exigencia en temas de seguridad y protección de datos.

- ***Cloud* Privado (Interno):** Forma de implementación caracterizada por el suministro por parte del proveedor, de entornos virtualizados que pueden ser implementados, usados y controlados por la misma empresa contratante del servicio. Esto indica no solo que la

solución *Cloud* puede ser administrada por la organización contratante, por el proveedor o por un tercer actor; sino que puede existir en las instalaciones propias del cliente o fuera de las mismas.
Como características propias de esta forma de implementación se enumeran las siguientes:

- Reducido plazo de tiempo para la puesta en servicio y una alta flexibilidad en la asignación de recursos.
- Al contrario que el *Cloud* público, requiere de inversión económica para la implementación de la solución contratada.
- Lleva asociados sistemas y bases de datos locales.
- Ofrece la posibilidad de aprovechar el personal existente y las inversiones en sistemas de información realizadas con anterioridad.
- Implica más especificidad en la solución adquirida, ya que está diseñada para ajustarse a las necesidades propias de la empresa contratante.
- Permite disponer de un control total de la infraestructura, de los sistemas y de la información corporativa tratada por éstos.
- Facilita el control y la supervisión de los requisitos de seguridad y protección de la información almacenada.

- ***Cloud* de Comunidad:** Se trata de *Clouds* utilizados por distintas organizaciones cuyas funciones y servicios sean comunes, permitiendo con ello la colaboración entre grupos de interés. Ejemplos de esta forma de implementación son los *Clouds* de comunidades de servicios de salud (en inglés, *healthcare community cloud*) para facilitar el acceso a aplicaciones e información crítica de carácter sanitario, y los *Clouds* de comunidad gubernamentales (en inglés, *go-*

vernment community cloud) para facilitar el acceso a recursos de interoperabilidad entre organismos públicos y Administraciones Públicas.

Al analizar un *Cloud* de comunidad, se debe considerar que, en principio, sus fortalezas y debilidades se sitúan entre las del privado y las del público. En general, el conjunto de recursos disponibles con un *Cloud* de comunidad es mayor que en el privado, con las ventajas evidentes que ello conlleva en términos de elasticidad. Sin embargo, la cantidad de recursos es menor que los existentes en una solución de *Cloud* público, limitando la elasticidad respecto a dicho *Cloud* público. Por otra parte, el número de usuarios de este tipo de nube es menor que los de la nube pública, lo que la dota de mayores prestaciones en cuestiones de seguridad y privacidad.

- ***Cloud* Híbrido:** Forma de implementación cuya infraestructura *Cloud* (en la nube) se caracteriza por aunar dos o más formas de *Clouds* (privado, comunitario o público), los cuáles continúan siendo entidades únicas interconectadas mediante tecnología estandarizada o propietaria, tecnología que permite la portabilidad de datos y aplicaciones (ej. el rebalanceo de cargas entre nubes). Una entidad que emplee esta forma de implementación se podría beneficiar de las ventajas asociadas a cada tipo de *Cloud*, disponiendo con ello de una serie de características adicionales, tal y como se muestra a continuación:

  - Ofrece una mayor flexibilidad en la prestación de servicios de TI, al mismo tiempo que se mantiene un mayor control sobre los servicios de negocio y de datos.

- Con una solución de *Cloud* híbrido, al igual que en los casos detallados anteriormente, se consigue una rápida puesta en servicio.
- Implica mayor complejidad en la integración de la solución *Cloud*, como consecuencia de ser una solución que se compone de dos formas distintas de implementación de servicios en la nube.
- Permite integrar las mejores características de las dos formas de implementación *Cloud*, en cuanto al control de los datos y a la gestión de las funciones básicas de la entidad.
- Posibilita la selección por parte del proveedor, de infraestructura escalable y flexible, permitiendo una alta agilidad en el redimensionamiento de la solución.
- Permite el control interno de los servicios *Cloud* desde la propia entidad.

4. Ventajas del Cloud Computing

Las líneas estratégicas de competitividad de las pymes se fundamentan en el desarrollo de determinados ejes como la comercialización, la internacionalización, la eficiencia productiva, la capacitación del capital humano, la eficiencia financiera, la calidad o el grado de implantación de las tecnologías e innovación.[59]

En este contexto, el *Cloud Computing* puede consolidarse como un instrumento acelerador para que una empresa logre evolucionar en su competitividad. El *Cloud* se perfila como una alternativa ágil y eficiente para que

[59] Consultas en internet: www.atc.ugr.es/pages/docencia/no_reglada/tendencias_ic/media/_doc, (20/10/2013).

las pymes puedan acceder a soluciones y servicios tecnológicos que permitan optimizar su negocio y lograr una mejora significativa en sus operaciones y, por ende, lograr una notable mejora competitiva en el mercado. El Cloud Computing proporciona un acceso más rápido, flexible y económico a tecnologías y servicios que mejorarán la competitividad de las empresas.

Las organizaciones podrán acceder a infraestructuras y soluciones tecnológicas que permitirán optimizar su cadena productiva y de suministro (soluciones de automatización de procesos, plataformas de gestión financiera, infraestructuras físicas, etc.), podrán acceder a servicios de *outsourcing* o tercerización más sofisticados y automatizados, agilizarán la captación de profesionales cualificados a través de las redes sociales profesionales, podrán acceder a plataformas de conocimiento y formación en la nube, tendrán disponibles soluciones para implementar estrategias de marketing y gestión personalizada de clientes o podrán operar en mercados electrónicos internacionales y ofrecer sus productos y servicios a través de entornos de comercio electrónico.

Todas estas oportunidades de mejora, que ya se desarrollaban sin el *Cloud Computing*, se han vuelto más accesibles y fáciles de implementar para todas las empresas, en términos operativos y de coste: el *Cloud Computing* supone y supondrá un efecto acelerador en el acceso de las empresas, y en especial de las pymes, a instrumentos y servicios que redundarán en una mejora de competitividad en el corto plazo.

Según diversos estudios, las empresas que apuestan por la implementación de modelos tecnológicos basados en *Cloud Computing* adquieren un conjunto de ventajas operacionales inmediatas en el despliegue y consumo de los servicios tecnológicos necesarios para su negocio: la eficiencia en costes (se puede llegar a lograr un ahorro del 50% de costes tecnológicos respecto del modelo tradicional), el ajuste de la inversión, la agilidad en el

despliegue de nuevos procesos, productos y servicios y la focalización de los recursos en los procesos de valor de la compañía.

Aunque con carácter general la integración de servicios *Cloud* implica todas estas ventajas y oportunidades para la competitividad de las empresas, son las áreas de tecnología las que asumen el mayor impacto, beneficios y riesgos con la adopción de este modelo.

A continuación, se presenta un conjunto de ventajas y oportunidades que redundan de forma específica en el departamento de TI de una compañía:

- Gracias al modelo de pago por uso, el coste asociado a los servicios es variable e inferior al incurrido con el uso de tecnología tradicional. La importancia del concepto *on-demand* asociado al uso de soluciones en la nube, radica en que, a diferencia de lo que ocurre en el caso de la infraestructura tradicional, el suscriptor del servicio de *Cloud Computing* tan sólo paga por el uso realizado, reduciéndose sustancialmente los costes fijos y las inversiones asociadas a los recursos TI.
- Los clientes del Cloud Computing no tienen que ser necesariamente dueños de la infraestructura usada, evitando así asumir las inversiones de capital. Esto se consigue mediante la contratación de los servicios ofertados por un proveedor o intermediario, el cual disponga de soluciones dentro de su catálogo de servicios.
- Adicionalmente a la reducción de los gastos asociados a la compra de nuevas herramientas informáticas y a la renovación de licencias de las mismas, el uso de soluciones Cloud supone un ahorro de costes de personal, ya que no es necesario disponer de un gran departamento de TI en el organigrama interno de la empresa, con lo

que gran parte del personal encargado de la gestión de los recursos de TI puede reubicarse en otras áreas de la compañía.

- El precio de los servicios Cloud es competitivo por efecto de las economías de escala generadas gracias a ciertas características inherentes al modelo Cloud como son la escalabilidad, el autoservicio bajo demanda y el pago por uso.
- Las organizaciones pueden concentrar todos sus esfuerzos en su negocio, ya que pueden encomendar al proveedor toda la responsabilidad y la gestión de competencias de la entidad asociadas a TI.
- El despliegue de los sistemas y servicios Cloud contratados al proveedor por parte de los clientes es rápido y sencillo, permitiendo a las empresas usuarias optimizar sus procesos productivos y sus costes.
- Debido a la alta flexibilidad de las soluciones *Cloud* y su agilidad en la escalabilidad a medida que aumentan los requerimientos de los clientes, la solución *Cloud* contratada puede redimensionarse fácilmente para cubrir dichas necesidades.
- Se pueden liberar fácilmente (interrumpiendo el pago por uso y dándose de baja al cliente en los sistemas del proveedor) los recursos de TI una vez que dejen de ser utilizados, así como se puede mantener la configuración de los mismos almacenada en los sistemas propios del cliente, para un posible nuevo uso en el futuro.
- Gracias al escenario *Cloud*, el cliente siempre dispone para su uso, de la última actualización tecnológica de la infraestructura, sistemas, configuración, aplicaciones, etc.; lo que elimina el riesgo de pérdida de competitividad por obsolescencia tecnológica en el tratamiento de la información, y le permite disponer de recursos tecnológicos suficientes, como para que los requerimientos técnicos no

sean un obstáculo a la hora de ofrecer nuevos productos y servicios, abrir nuevas líneas de negocio o modificar los modelos de gestión internos.

- Los grupos de usuarios del *Cloud* y las distintas comunidades asociadas a ellas que comparten recursos dentro de una misma nube, permiten impulsar la innovación y la mejora continua de los productos y servicios dispuestos por el proveedor.
- Adicionalmente, la retroalimentación aportada por los primeros usuarios de la soluciones Cloud, permite identificar y desarrollar rápidamente las modificaciones tecnológicas requeridas, para cubrir los puntos débiles detectados.
- Como consecuencia de la particularidad de la tecnología *Cloud*, de la capacidad de abstracción del cliente respecto a la gestión de sus recursos de TI, el mantenimiento puede ser sencillo y seguro, siempre y cuando la solución de *Cloud Computing* contratada implique que el entorno *Cloud* sea gestionado por el proveedor, quien dispone de las últimas técnicas y tecnologías en materia de seguridad y protección de datos.
- Los proveedores de servicios *Cloud* disponen de sistemas duplicados que reducen la posibilidad de pérdida de información o de servicio en caso de un desastre. Los proveedores de soluciones en la nube, ofrecen tanto soporte frente a problemas en cualquier momento del año, como redundancia de sus sistemas para asegurar una mayor disponibilidad de la información que gestionan.
- Gracias a las características específicas del *Cloud Computing*, a pesar de que el usuario disponga de acceso a varios servidores, tan sólo resulta necesario solicitar un único acceso, no requiriéndose completar la configuración de la totalidad de servidores.

- El acceso a los recursos informáticos a través de Internet, permite que varias personas puedan trabajar a la vez en un mismo documento en tiempo real, mejorando con ello la productividad y fomentando la comunicación entre el personal interno de la organización. Además, el acceso ilimitado que ofrece el *Cloud Computing* aumenta la flexibilidad de la empresa, y permite a sus empleados disponer de los recursos tecnológicos necesarios para trabajar a distancia, mejorando también con ello la productividad del personal de la entidad.

Todas las ventajas del *Cloud Computing* presentadas son aplicables, en términos generales, a cualquier tipo de empresa. Sin embargo, la dimensión o sector en el que opera una compañía incide en la tipología de servicio y modelo *Cloud* que debe integrar para maximizar los beneficios de su inversión. Así, para analizar el impacto y beneficios que las soluciones *Cloud* aportan a cada tipo de empresa es conveniente segmentarlas según dos aspectos característicos: su tamaño y sector.[60]

En función del tamaño y capacidad de la empresa las alternativas de *Cloud* público parecen las más adecuadas y efectivas, mientras que compañías grandes con mayores recursos y volumen de gestión suelen apostar por la implementación de nubes privadas o híbridas.

En cuanto a la división sectorial, para cubrir las necesidades propias de cada potencial cliente, los proveedores recopilan los procesos típicamente desarrollados por las empresas de cada sector organizativo, y desarrollan las funcionalidades necesarias para cubrir los requerimientos de las entidades del sector; desarrollando con dichas funcionalidades, las correspondientes soluciones *Cloud* específicas para el sector en cuestión. Igual-

[60] URUEÑA, Alberto, op. cit., pág. 31.

mente, la naturaleza del negocio del sector y las necesidades de procesamiento tecnológico, determinan las principales ventajas que el *Cloud* puede aportar en dicho sector.[61]

5. Desventajas y Riesgos del Cloud Computing

Como desventajas podemos citar las siguientes:[62]

- No controlar la localización de los datos. Un servicio en la nube puede almacenar los datos en distintas localizaciones y el usuario del servicio no tiene control sobre dónde están sus datos. Esta falta de control puede suponer un problema dependiendo del carácter de los datos y la legislación de cada país. Por ejemplo, existen verdaderos problemas para poner datos médicos sobre pacientes en la nube o datos de organizaciones gubernamentales que sean catalogados como clasificados, ya que las leyes de cada país con respecto a este tipo de datos son muy estrictas.
- El usuario debe preocuparse por los acuerdos de niveles de servicios. La única herramienta que el usuario posee para garantizar el servicio que está contratando son los acuerdos de niveles de servicio, con lo que se medirá la calidad del mismo.
- Inversión en comunicaciones. Otra de las desventajas de utilizar servicios en la nube es que las comunicaciones con la nube deben ser lo suficientemente fiables como para garantizar el acceso a los servicios contratados. Además de la disponibilidad también debemos asegurarnos que el caudal que tenemos de acceso a los servi-

---

[61] Ibidem.

[62] MORA PÉREZ, José Juan, *Capacity Planning* IT: Una aproximación práctica, (Madrid, 2012), Pág. 448.

cios en la nube garantizan que el acceso al servicio tiene la calidad necesaria para el desarrollo del negocio. Las comunicaciones externas son sensiblemente más caras que las comunicaciones internas. Al tener servicios en la nube, una organización podría tener que aumentar los caudales de acceso a la misma con el consiguiente gasto.

- La información podría ser accedida por terceros. La gestión del acceso a nuestra información se la delega a un proveedor de servicios en la nube, un problema de seguridad en dicho proveedor puede provocar que los datos alojados en la infraestructura del proveedor pudieran ser accesibles por otras personas. Los usuarios deben ser conscientes de este riesgo y lo que supondría que terceros tuvieran acceso a su información.
- Cuidado con las plataformas para desarrollar aplicaciones. Al desarrollar aplicaciones en Plataformas como un servicio, podemos encontrar el problema de la migración, tanto de los datos, como del código a otro proveedor. Muchos proveedores ofrecen plataformas propias de desarrollo de aplicaciones por lo que todo que se desarrolla en las mismas, muy rara vez se pueden migrar a otras.
- Los recursos no son infinitos. Una de las características de los servicios en la nube es la elasticidad de los recursos. El proveedor ofrece recursos acorde a las necesidades, pero se debe ser conservador con esta idea, ya que un proveedor de servicios no puede dar recursos ilimitados y se pueden encontrar situaciones donde las necesidades de negocios requieran más recursos de los que el proveedor pueda suministrar, quedando atrapados en un servicio que costará mucho esfuerzo migrar a otro proveedor.

Por su parte, se identifican como principales, siete riesgos en el área del Cloud Computing:

- La confianza del proveedor: Externalizar sus aplicaciones y datos corporativos conlleva hacerlo con alguien de total confianza, que le asegure la calidad del servicio, los términos de confidencialidad de su relación contractual, etc.
- Conformidad legal: Al final, el responsable en caso de infracción es el propietario de la información. Por ello, los proveedores de *Cloud Computing* deberán estar abiertos a cualquier tipo de auditoría externa y a tomar y cumplir toda medida que sea necesaria para garantizar el cumplimiento de la normativa y, con ello, la seguridad de sus clientes.
- Localización de los datos: Es uno de los puntos fuertes del *Cloud Computing* pero también uno de sus riesgos. Poder acceder a los datos en cualquier momento, independientemente de dónde estén localizados, debe estar garantizado para el cliente.
- Protección de la información: Porque se comparten recursos pero esto no puedo ir en menoscabo de la confidencialidad de los datos del cliente, que deberá estar garantizada en todo momento.
- Recuperación: Desconocer la localización de la información no puede implicar jamás que no existan las medidas necesarias de seguridad y replicación para garantizar su recuperación en caso de desastre o pérdida de los mismos.
- Colaboración con la Justicia: Acatamiento de las leyes de protección y seguridad de la información, independientemente de que ésta varíe según las normas propias del país donde se localicen los datos y aplicaciones del usuario.

- Una relación “para toda la vida”: La sostenibilidad del proveedor tiene que estar garantizada. Fusiones, quiebras, cualquier cambio en su negocio no puede dejar “indefenso” al cliente y, por ello, se establecerá un compromiso de continuidad a largo plazo en la relación en los propios términos del contrato.

6 – Seguridad y Privacidad de los Datos

Los datos residen en sistemas tecnológicos que se encuentran fuera del alcance del *firewall* de la empresa. Por este motivo, existe una gran reticencia al uso de la tecnología *Cloud* en las empresas privadas y organizaciones públicas, en los sistemas de la entidad que contienen información crítica para la misma.

La seguridad y privacidad de la información que se traslada a la nube es uno de los aspectos más importantes para las compañías. Es evidente que los servicios de *Cloud Computing* prestados por el proveedor, implican un determinado nivel de confianza por parte de los contratantes del servicio en dichos proveedores, ya que se delega en un operador externo todas las acciones y la responsabilidad de la información de los datos corporativos y su control y gobierno. Además, dependiendo de la naturaleza de los procesos y datos externalizados, la casuística es aún más compleja al condicionarse la contratación y operación por el marco de todo contexto contractual entre el suscriptor y el proveedor, que debe contextualizarse en un marco de confianza fundamentado en el cumplimiento de estándares y políticas de seguridad por parte de ambas partes. El proveedor de servicios *Cloud* debe garantizar el cumplimiento de los procesos y técnicas exigidas y certificadas por dichos estándares, mientras que el suscriptor debe aplicar una política adecuada de control y gestión del riesgo tecnológico.

Dentro de esta política de control y gestión del riesgo tecnológico, y previamente a la adopción de modelos de computación en la nube en una organización, es necesario realizar un estudio de la implementación, donde se tengan en cuenta aspectos de seguridad y continuidad de negocio.

El cumplimiento normativo será uno de los factores clave a la hora de llevar a cabo dicho estudio de implementación.

Como paso inicial, es necesario identificar la normativa aplicable. Para ello, es imprescindible analizar factores como los siguientes:

- Información que se desea llevar a la nube.
- Sector de la compañía.
- Familia de servicio que se desea contratar.
- Criticidad del proceso de negocio que soportará la nube.

En función de los requisitos establecidos por las diferentes normativas que sean de aplicación, se elaborarán los requisitos normativos, con los que se validará si un determinado proveedor puede considerarse como una alternativa válida para ofrecer el servicio deseado.

El cliente, como responsable de los datos, tiene la obligación de exigir que el proveedor de servicios establezca todas las medidas de seguridad, técnicas y organizativas, que se requieran.

Se mantiene así la responsabilidad del cliente sobre la seguridad de los datos. En este sentido, la externalización, lejos de evitar problemas por delegar la seguridad de los datos en un tercero, introduce un riesgo de cumplimiento para el responsable de los datos, quedando a expensas del buen hacer del proveedor.

Adicionalmente a los requisitos normativos y al riesgo de cumplimiento, la propia organización deberá analizar qué requisitos de seguridad considera necesario aplicar.

Los requisitos de seguridad deben estar acordes con:

- La política de seguridad de la compañía.
- El nivel de seguridad requerido en función del tipo de información.
- Los requerimientos de la compañía en cuanto a la disponibilidad del servicio.
- El proceso de negocio al que vaya a dar soporte el servicio.
- Disponibilidad del sistema y tiempos de recuperación.
- Gestión y comunicación de incidentes de seguridad.
- Borrado seguro.
- Exportación de los datos almacenados.

Una vez analizado el nivel de cumplimiento de los requisitos normativos y de seguridad por parte del proveedor, la compañía debe ser consciente de que el carácter externalizado y las particularidades del modelo de computación en la nube supondrán en todo caso una serie de riesgos de seguridad.

Los riesgos de seguridad deberán ser analizados por negocio y asumidos por el máximo responsable del proceso de negocio al que se vaya a dar soporte. Por ello, se deben requerir explícitamente por contrato las medidas de seguridad a implementar.

Algunas de estas medidas son:

- Documento de seguridad.

- Copias de respaldo y procedimientos de restauración de datos.
- Control de acceso.
- Identificación y autenticación.
- Gestión de incidencias.
- Gestión de soportes de almacenamiento.
- Comunicación cifrada de la información.
- Registro de accesos a datos de nivel alto.

A continuación, se muestran algunos ejemplos de riesgos de seguridad que podrían ser de aplicación ante una eventual contratación de servicio de *Cloud Computing*:[63]

- Fuga de información provocada por ataques a la plataforma.
- Incapacidad de migración de los datos ante la finalización del servicio.
- Borrado no seguro de la información.
- Incidencias/ incidentes no comunicadas.
- Pérdida de disponibilidad de la información y/o del servicio.
- Pérdida de información por falla del proveedor.

[63] URUEÑA, Alberto, op. cit., pág. 65.

CAPÍTULO VIII

BlackBerry – Casos Exitosos de Aplicación

Sumario: 1. El concepto de Seguridad para BlackBerry; 2. Principales Productos y Servicios Empresariales; 3. Prestaciones para Empresas; 4. Caso 1: Cablevisión S.A.¸5. Caso 2: Banco de la Provincia de Córdoba S.A.; 6. Caso 3: Diarco; 7. Caso 4: Ministerio de Desarrollo Social.

1. El concepto de seguridad para BlackBerry

Dado que cada vez es más frecuente que los empleados trabajen fuera del entorno seguro de las empresas, el riesgo de que la seguridad de los datos se vea comprometida y de que la red corporativa sea accedida por usuarios malintencionados va en aumento. Entre las amenazas a la seguridad se encuentran los virus, troyanos, gusanos y otros tipos de programas maliciosos que se cargan en el dispositivo a través de una aplicación móvil sin que el usuario lo note, y la pérdida o el robo de equipos que tienen almacenada información confidencial.[64]

---

[64] Consultas en Internet: www.ar.blackberry.com/business/topics/security.html, (22/10/2013).

Ciertas mejores prácticas permiten garantizar la seguridad de la solución de movilidad:

- Asegurarse de que la estrategia de seguridad inalámbrica contemple los dispositivos móviles y los datos almacenados en ellos, como también las comunicaciones realizadas desde y hacia ellos
- Desarrollar una política de seguridad a nivel empresarial, comunicarla, aplicarla y verificar su cumplimiento
- Procurar que la política de seguridad inalámbrica se integre con sus estándares de seguridad actuales
- Desarrollar un plan para medir, auditar y llevar un registro del rendimiento de la política de seguridad
- Brindar a los administradores de TI la capacidad para establecer, hacer cumplir y actualizar las configuraciones de los dispositivos inalámbricos a través de políticas que permitan realizar un control exhaustivo de todos los dispositivos.

La plataforma BlackBerry es una plataforma móvil muy segura diseñada para mantener a salvo los datos corporativos en *Smartphones* BlackBerry. Las prestaciones de seguridad integral y un conjunto de herramientas administrativas en constante ampliación han otorgado a los productos BlackBerry la confianza de algunas de las organizaciones más seguras del mundo. Dichas prestaciones de seguridad también han convertido la solución BlackBerry en líder mundial en certificaciones de seguridad móvil.

Una cuestión de seguridad primordial ahora mismo es cómo proteger los dispositivos cuando se utilizan para fines personales y profesionales. *Research In Motion* (RIM) continúa desarrollando herramientas que proporcionan tranquilidad a las empresas. La tecnología BlackBerry *Balance* ofrece protección para redes y datos de la empresa sin comprometer la experiencia

del usuario final. Esto significa que las empresas pueden proteger sus activos a la vez que permiten que los empleados instalen sus aplicaciones favoritas.[65]

2. Principales productos y servicios empresariales

Entre los productos y servicios empresariales ofrecidos por la empresa, se destacan los siguientes:

a. *BlackBerry Enterprise Service* 10: Es una plataforma de seguridad y administración de dispositivos personales y corporativos que opera con sistema operativo BlackBerry, BlackBerry 10, iOS o Android. Permite obtener el nivel de control que se necesita al tiempo que se ofrece a los usuarios la experiencia que desean.

Constituye una verdadera solución multiplataforma para la administración de la movilidad empresarial (*Enterprise Mobility Management*, EMM).[66]

Es ideal para empresas de cualquier tamaño o industria que buscan una interfaz simple de administración de teléfonos inteligentes y *tablets* BlackBerry.

Entre sus principales características se destacan las siguientes:

- *BlackBerry Enterprise Service* 10 permite a las empresas gestionar complejas flotas de dispositivos móviles.

---

[65] Consultas en Internet: www.es.blackberry.com/business/topics/security/overview.html, (22/10/2013).

[66] Consultas en Internet: www.ar.blackberry.com/business/software/bes-10.html, (23/10/2013).

- Posibilita la gestión de múltiples dispositivos diferentes por cada usuario, tanto los de propiedad de la empresa como los de propiedad personal
- Satisface toda la gama de necesidades de seguridad; desde un nivel básico hasta las necesidades de alta seguridad y control de entornos gubernamentales y sectores regulados.
- Gestión de todos los dispositivos y usuarios a través de una sola plataforma y consola de administración. Puede incluso usar BlackBerry *Enterprise Service* 10 para gestionar su entorno de *BlackBerry Enterprise Server o BlackBerry Enterprise Server Express*.

b. *Secure Work Space*: Es una nueva opción de contenedorización, envoltura de aplicaciones y conectividad segura que proporciona un nivel mayor de control y seguridad para dispositivos iOS y Android, todo ello gestionado a través de una sola consola de administración de *BlackBerry Enterprise Service* 10.

Las aplicaciones administradas permanecen seguras y separadas de las *apps* y los datos personales, ofreciendo una *app* integrada de correo electrónico, calendario y contactos, un navegador seguro en el nivel de la empresa y una función segura de visualización y edición de adjuntos mediante *Documents To Go*.[67]

Se necesita autenticación de usuario para acceder a las *apps* seguras, y los datos de trabajo no pueden compartirse fuera del espacio de trabajo seguro.

[67] Ibidem.

c. *BlackBerry Balance*: *BlackBerry Balance* ofrece a sus empleados la libertad y la privacidad que desean para su uso personal, y al mismo tiempo proporciona la seguridad y la gestión que necesita para el uso empresarial. Aúna lo mejor de ambos mundos, incorporado perfectamente en cada *Smartphone BlackBerry* 10 y gestionado a través de *BlackBerry Enterprise Service* 10.

Las apps y la información de trabajo quedan separadas de las personales, y el usuario puede cambiar de su espacio personal a su espacio de trabajo con un simple gesto.

El espacio de trabajo está completamente cifrado, administrado y seguro, lo que permite a las organizaciones proteger las aplicaciones y contenidos críticos.[68]

Entre sus ventajas se pueden mencionar las siguientes:

- Separación segura de datos personales y empresariales: Permite mantener la información personal separada y la información empresarial altamente protegida admitiendo el acceso al dispositivo BlackBerry personal mientras está bloqueado su uso empresarial.
- Regulación de aplicaciones de terceros: Permite restringir el acceso de los empleados a datos empresariales a través de aplicaciones de redes sociales, e impide que copien y peguen de una aplicación empresarial a una personal.
- Gestión remota de *Smartphones*: Posibilita borrar información empresarial de dispositivos BlackBerry de forma remota manteniendo intacta la información personal.

[68] Ibidem.

- Facilidad de uso: Se requiere una mínima formación de los usuarios y las notificaciones visuales en el *Smartphone* BlackBerry alertan a los usuarios cuando emprenden acciones que entran en conflicto con las políticas de TI establecidas.
- Soporte de usuario más amplio: Permite respaldar a más miembros de una organización con la posibilidad de segregar y controlar el uso empresarial frente al personal.

d. *BlackBerry Enterprise Server*: Pensado para satisfacer las necesidades de los sectores empresarial y gubernamental, BlackBerry *Enterprise Server* es la solución ideal para empresas que tienen un servidor *in situ* y que necesitan un alto nivel de control de TI.
Se puede ejecutar junto con *BlackBerry Enterprise Server Express* en aquellas empresas en que solo un pequeño grupo de usuarios necesita funciones avanzadas de administración de TI.[69]
Se mencionan sus características más relevantes:

- Hasta dos mil usuarios por servidor
- Posibilidad de agregar tantos servidores como sea necesario
- Compatibilidad con las plataformas de correo electrónico *IBM Lotus Domino, Microsoft Exchange* y *Novell GroupWise*
- Más de quinientas políticas de TI
- Encriptación *Advanced Encryption Standard* (AES) o Triple *Data Encryption Standard* (Triple DES)

[69] Consultas en Internet: www.ar.blackberry.com/business/software/bes.html, (23/10/2013).

- Separación y protección de la información corporativa y personal almacenada en los teléfonos inteligentes BlackBerry
- Posibilidad de eliminar, en forma remota, la información corporativa almacenada en los teléfonos inteligentes BlackBerry sin modificar la información personal
- *BlackBerry Administration Service* permite planificar actualizaciones de dispositivos, aplicaciones y políticas de TI
- Las políticas de TI permiten administrar grupos y configuraciones de usuarios
- Visualización de las principales métricas desde el teléfono inteligente BlackBerry
- Desarrollo de aplicaciones personalizadas a través de BlackBerry *Administration*
- Administración inalámbrica de aplicaciones
- Java, tecnología *push* y otras herramientas de desarrollo basadas en la web.

e. *BlackBerry Enterprise Server Express:* Software gratuito para empresas en crecimiento que permite movilizar plataformas de correo electrónico.

Sincroniza en forma inalámbrica los teléfonos inteligentes BlackBerry con *Microsoft Exchange* o *IBM Lotus Domino*. BlackBerry *Enterprise Server Express* ofrece las funciones empresariales avanzadas que distinguen a los teléfonos inteligentes BlackBerry sin costos de licencias de *software* ni licencias de usuario adicionales.

Además, BlackBerry *Enterprise Server Express* incluye la tecnología BlackBerry *Balance* y compatibilidad con *Microsoft Office* 2010.[70]

Es ideal para pymes que buscan funciones avanzadas de movilidad a un precio más bajo o que quieren conectar teléfonos inteligentes BlackBerry personales a la red corporativa.

Sus características más destacadas son:

- Hasta dos mil usuarios en un servidor dedicado de *IBM Lotus Domino*.
- Hasta setenta y cinco usuarios en su servidor actual de *Microsoft Exchange Server* o de *Windows Small Business Server*.
- Posibilidad de agregar servidores a cualquier configuración para admitir hasta dos mil usuarios por servidor.
- Borrado de datos o bloqueo de teléfonos inteligentes BlackBerry perdidos o robados.
- Prevención de acceso no autorizado a la información corporativa (uso de contraseñas para desbloquear los dispositivos).
- Implementación de configuraciones de seguridad (como bloqueo de *Bluetooth*) en forma inalámbrica.
- Más de setenta y cinco políticas de TI para controlar la implementación de teléfonos inteligentes BlackBerry.
- Métodos de encriptación *Advanced Encryption Standard* (AES) y *Triple Data Encryption Standard* (Triple DES).

---

[70] Consultas en Internet: www.ar.blackberry.com/business/software/besx.html, (23/10/2013).

- Consola de administración basada en la web BlackBerry *Administration Service.*
- Administración de teléfonos inteligentes de la empresa (incluye el restablecimiento de contraseñas y la configuración de políticas de TI en forma inalámbrica).
- Implementación y administración de aplicaciones en forma inalámbrica y planificación de actualizaciones de dispositivos, aplicaciones y políticas de TI.
- Posibilidad de iniciar sesión en BlackBerry Web *Desktop Manager* desde cualquier computadora.
- Los usuarios pueden borrar los datos y bloquear o deshabilitar su propio teléfono inteligente en caso de pérdida o robo.
- Los usuarios pueden realizar copias de seguridad y restaurar los datos, o cargar nuevas aplicaciones en su teléfono inteligente BlackBerry.

f. BlackBerry *Messenger*: BlackBerry *Messenger* (BBM) es una aplicación de mensajería instantánea creada para los teléfonos inteligentes Blackberry y a partir del 21 de octubre de 2013, para smartphones con sistema operativo iOS, Android.
Características principales:

- Comunicación en tiempo real
- Permite enviar y recibir mensajes con hasta dos mil caracteres en cuestión de segundos. Cuenta con indicadores de mensajes entregados y leídos.
- Socialización con aplicaciones como Facebook, Twitter, BlackBerry *Travel* y BlackBerry *World*.

- Posibilidad de cambiar del chat de BBM a una conversación de video de BBM con solo un toque. La nueva función de intercambio de pantallas permite mostrar fotografías o el navegador, o revisar un documento de negocios. Hasta se puede compartir la vista de la cámara.
- Toda la información que el usuario necesita está disponible en el manual del usuario de BlackBerry *Messenger*: conceptos básicos, accesos directos, funciones como crear grupos o compartir tu ubicación, PIN BlackBerry y más.
- Totalmente personalizable. Se puede optar desde una imagen o tu avatar animado, hasta un mensaje personal y los colores de las burbujas del chat para crear una propia experiencia de BBM.
- Creación de la red propia. Permite escanear códigos de barras y compartir el PIN para agregar amigos a BBM. Luego se pueden crear grupos de BBM para enviar mensajes a varios contactos al mismo tiempo.
- Compartir fotos, videos, notas de voz y archivos de hasta seis MB.

g. *BlackBerry Enterprise Instant Messaging:* Permite y amplía la productividad mediante la movilización de soluciones de mensajería instantánea de escritorio, optimizando la comunicación y la colaboración con mensajería instantánea segura en tiempo real entre dos o más personas. Facilita iniciar al instante una conversación de mensajería instantánea entre dos o más personas o unirse a un chat de grupo para comunicarse rápida y eficazmente y acelerar la toma de decisiones.

Permita conexiones más rápidas, especialmente cuando los plazos son críticos, con una experiencia integrada que eleva el texto a voz para realizar conferencias con un cliente unificado.

Inicia fácilmente un chat de mensajería instantánea donde se puede compartir contenidos por correo electrónico. Eleva el chat a una llamada telefónica con un simple clic, sin necesidad de marcar un número.

Todas las comunicaciones son confidenciales y privadas ya que los mensajes enviados a través del cliente de Enterprise IM están cifrados de extremo a extremo.

3 - Prestaciones para empresas

Una movilidad empresarial segura resulta esencial para su empresa hoy día. La seguridad y capacidad de gestión de las soluciones BlackBerry® han hecho de los dispositivos BlackBerry el estándar de oro para las empresas.

Entre las principales prestaciones empresariales de BlackBerry se pueden mencionar las siguientes:

- **Cifrado de datos de extremo a extremo:**

BlackBerry *Enterprise Solution* ofrece dos opciones para el cifrado de transporte. De forma predeterminada, BlackBerry *Enterprise Service* 10 utiliza el algoritmo más seguro que admiten BlackBerry *Enterprise Service* 10 y los *Smartphones* BlackBerry para el cifrado de capa de transporte de BlackBerry.

BlackBerry *Enterprise Service* 10 y un *Smartphone* BlackBerry generan una clave de cifrado de transporte de dispositivos utilizando un protocolo seguro autenticado bidireccionalmente. Esta clave se-

creta se almacena únicamente en la cuenta empresarial segura del usuario y en su *Smartphone* BlackBerry. El usuario del *Smartphone* puede regenerar la clave de forma inalámbrica en cualquier momento.

Los datos enviados al *Smartphone* BlackBerry son cifrados por BlackBerry *Enterprise Service* 10 utilizando una clave recuperada del buzón de correo del usuario. La información cifrada viaja de forma segura a través de la red hasta el *Smartphone* donde se descifra utilizando la clave almacenada en el dispositivo.

- **Aplicación y gestión de una sólida política de TI:**

BlackBerry *Enterprise Solution* extiende la seguridad empresarial al *Smartphone* y proporciona a los administradores herramientas para gestionar dicha seguridad. Por ejemplo, para proteger la información almacenada en *Smartphones* BlackBerry, un administrador puede requerir a los usuarios que protejan sus *Smartphones* con contraseñas y definan políticas sobre la longitud y la complejidad de las mismas. De forma predeterminada, si se introduce una contraseña de forma incorrecta diez veces, se borra la memoria del dispositivo.

El cifrado local de todos los datos (mensajes, entradas de la libreta de direcciones, entradas de calendario, notas y tareas) también se puede aplicar a través de la política de TI. Asimismo, los administradores de sistemas pueden crear y enviar comandos inalámbricos para cambiar de forma remota contraseñas de *Smartphones* BlackBerry y bloquear o eliminar información de dispositivos perdidos o robados.

- **Seguridad de BlackBerry Enterprise Service 10:**

BlackBerry *Enterprise Service* 10 no almacena ningún correo electrónico ni datos. Para proteger los datos frente a accesos no autorizados, no hay zona de preparación entre el servidor y el *Smartphone* BlackBerry donde se descifran los datos.

La seguridad se mejora más si cabe permitiendo tan solo conexiones iniciadas salientes autenticadas a través del puerto 3101 del cortafuegos. No se permite tráfico entrante desde fuentes distintas del *Smartphone* BlackBerry o el servidor de correo electrónico, lo que implica la imposibilidad de ejecutar comandos no autorizados en el sistema.

- **Conexiones de navegador seguro:**

El servicio de conexión MDS de BlackBerry permite a usuarios acceder a contenido web, Internet o la intranet de su organización. También permite la conexión de apps de *Smartphone* a los servidores de aplicaciones de su organización o a los servidores de contenido para recuperar datos y actualizaciones. Autentica con Microsoft *Active Directory* en nombre de los usuarios, verifica las identidades y recupera los recursos en nombre de los usuarios.

Dependiendo de los requisitos de seguridad corporativos, si una app de terceros en un *Smartphone* BlackBerry puede acceder a servidores en Internet, puede configurar el servicio de conexión MDS de BlackBerry para que use HTTPS con el fin de proporcionar seguridad y autenticación adicional para la conexión.

- **Controles de acceso de las aplicaciones:**

Las apps de *Smartphones* BlackBerry requieren que los desarrolladores firmen y registren sus aplicaciones con BlackBerry. Esto incrementa la protección al proporcionar un mayor grado de control y previsibilidad de la carga y el comportamiento de las apps en los dispositivos.

La herramienta de autoridad de firmas BlackBerry puede ayudar a proteger el acceso a la funcionalidad y datos de apps de terceros permitiendo a los desarrolladores o administradores de la empresa gestionar el acceso a determinadas interfaces de programación de aplicaciones (API) confidenciales y almacenes de datos mediante el uso de software del lado del servidor y claves de firma públicas y privadas.

- **Seguridad:**

BlackBerry marca el estándar de calidad para la movilidad segura de punto a punto:

- Cubre todo el abanico de necesidades de seguridad, desde el nivel básico hasta los niveles muy altos de seguridad y control.
- Protege frente a posibles filtraciones de datos y el acceso de dispositivos no autorizados a activos empresariales.
- Cifrado de punto a punto que protege contra posibles interceptaciones.
- Aplicaciones y datos corporativos seguros en dispositivos personales.
- Garantiza a los usuarios finales su privacidad y libertad (a través de BlackBerry Balance)

- Gestión de movilidad empresarial en el nivel regulado; la opción de controles y configuraciones permite cumplir totalmente con los requisitos gubernamentales y de entornos regulados

- **Aplicaciones:**
  - La estructura de gestión de aplicaciones empresariales y de productividad de BlackBerry *World* permite mantener en marcha los negocios a un bajo costo.
  - A través de BlackBerry *Enterprise Service* 10, las empresas pueden gestionar y mantener sin problemas una tienda de aplicaciones empresariales (BlackBerry *World for Work*) en el espacio de trabajo de BlackBerry *Balance* para promover e instalar apps obligatorias y publicar aplicaciones recomendadas para los usuarios, tanto corporativos como personales.
  - Con BlackBerry *Balance* activado, los usuarios de BlackBerry 10 pueden acceder y descargar apps, juegos, vídeo y música a través de BlackBerry *World* y guardar todo ello en su espacio personal, de forma segura y separada de su vida laboral.
  - Controles de gestión de EMM de nivel regulado para *Smartphones* BlackBerry 10 para que cumplan con los requisitos de entornos regulados y gubernamentales.
  - Opción de *Secure Work Space* para dispositivos iOS y Android que ofrece uso de contenedorización, envoltura de aplicaciones y conectividad segura.
  - Conexión segura, detrás del cortafuegos, con dispositivos iOS y Android. No es necesaria una solución de VPN separada.

- Funciones mejoradas de reporte. Funciones de exportación que permiten un mayor análisis mediante herramientas estándar.
- Implementación en un solo servidor. Todos los componentes previos pueden ahora ejecutarse en el mismo servidor físico o virtual.
- Alta disponibilidad para garantizar un servicio ininterrumpido a los usuarios (BlackBerry, iOS y Android).
- Administración más rápida y sencilla con un solo inicio de sesión.

- **Soluciones móviles:**

Son numerosas las empresas en todo el mundo que aumentaron su productividad y optimizaron el negocio con las soluciones móviles brindadas por BlackBerry.

En los puntos siguientes de este capítulo se presentan casos exitosos en empresas destacadas de nuestro país.

4. Caso 1: Cablevisión S.A.

Cablevisión S.A. Argentina (Cablevisión) es una empresa que brinda servicios de TV paga, Internet de banda ancha y telefonía mediante una red única. Cuenta con unos 3.500.000 clientes en Argentina, Uruguay y Paraguay.

Desafío:

Cablevisión necesitaba mantenerse en comunicación con sus más de 5.000 técnicos de campo, que se encuentran constantemente en las ca-

lles y domicilios, instalando nuevos servicios, haciendo conexiones o reparando. Previamente, los técnicos utilizaban una aplicación inalámbrica con acceso a Internet para recibir órdenes de trabajo a través del móvil (WAP), pero había algunos detalles que generaban nuevos desafíos. Varias veces la comunicación se veía interrumpida por falta de conectividad en la prestadora del servicio inalámbrico. Esto generaba tiempo de espera para los clientes y pérdidas financieras para la compañía con desagradables resultados y consecuencias adversas para el negocio directamente.[71]

Cablevisión también necesitaba una solución que ayudara con la actualización del inventario en línea. Los técnicos anotaban en papel la lista de los materiales usados, que entregaban a una asistente para que ingresara los datos al sistema de la compañía. Esto, sumado a los posibles errores humanos, generaba demoras en la actualización de datos, y en el reabastecimiento del inventario de hasta 24 horas.

También, durante una visita los técnicos de campo necesitaban contactar al área de soporte para reactivar o conectar el servicio. Incurriendo en retrasos para los clientes que se quejaban insatisfechos.

Solución:

Cablevisión equipó a sus técnicos con unos tres mil quinientos teléfonos inteligentes BlackBerry, administrados utilizando cinco BlackBerry *Enterprise Servers*. También, desplegó la aplicación *Mobile* II por *Sensebyte,* miembro de la Alianza BlackBerry. La aplicación permite a los técnicos recibir órdenes de trabajo, actualizar el inventario remotamente y obtener soporte del área de servicio –todo desde la conveniencia de sus dispositivos Black-

[71] Consultas en Internet: www.ar.blackberry.com/content/dam/blackBerry/pdf/caseStudy/latinAmerica/es/CS_CaseStudy_Cablevision_SP_FINAL.pdf, (25/10/2013).

Berry. Con la app, los técnicos reciben la lista diaria de órdenes de trabajo para el día, junto con la confirmación del área de soporte de Cablevisión que el cliente estará en casa. Estos reportan en cada paso del servicio, por ejemplo, indicando que está “en tránsito” y cuando llega cambia el estado a “movilizando”, para reportar que está comenzando la tarea de reparación o instalación. La app ofrece un menú de opciones para dejar registrado los materiales utilizados.[72]

Esta opción también funciona fuera *off -line*, actualizando de forma automática la información en el servidor central una vez se restaura la conexión. Los técnicos, también pueden ver un mapa con la localización de sus clientes, utilizando la funcionalidad nativa de GPS del teléfono inteligente BlackBerry.

Si los técnicos necesitan asistencia adicional para llevar a cabo una reparación, la app les permite comunicarse con el área de soporte de Cablevisión. Cuando finalizan el trabajo, reciben rápidamente un número de serie que les permite de forma inmediata conectar un nuevo servicio o reconectar uno existente.

Antes los técnicos tenían que llamar al área de soporte para activar un servicio y esperar en casa del cliente a un representante de soporte que les ayudara. Ahora, la app BlackBerry les da el número de serial en tiempo casi real, y el servicio es conectado en minutos.

Beneficios de Cablevisión:

La solución de BlackBerry ha mejorado enormemente los servicios técnicos e instalaciones diarias de Cablevisión. El nivel de servicio es mucho mejor y el tiempo necesario para cada trabajo ha disminuido.

---

[72] Ibidem.

Las llamadas al centro de servicio han disminuido significativamente, ahorrando tiempo tanto para los técnicos como para el personal de soporte. Y la compañía utiliza, ahora menos papel para dar soporte a sus técnicos pues los archivos se mantienen digitalmente.

La app Mobile II ayuda a los técnicos a trabajar todo el día sin interrupción en modalidad en línea u off-line si se interrumpe el servicio. Asimismo, la opción de actualización automática del inventario permite llevar un mejor control de sus existencias, manteniendo el inventario siempre al día y bien abastecido, previniendo cualquier retraso de servicio al cliente por falta de materiales. El inventario es actualizado rápidamente, y los datos son más exactos, que cuando se hacía en notas escritas a mano.

La solución BlackBerry permite administrar una gran logística técnica de una forma eficiente, rápida y conveniente, encontrando mejoras significativas en el área técnica, el área administrativa y hasta en el área de servicio al cliente.

Al combinar la infraestructura de Blackberry Enterprise Server con la aplicación Mobile II, Cablevisión ha efectuado una reingeniería de procesos internos, creando una operación más eficiente a través de la empresa. Considera que la solución aportada por BlackBerry es flexible y altamente escalable, convirtiéndose es una pieza clave en la forma de adaptarse a un mundo que evoluciona tecnológicamente muy rápidamente.

5. Caso 2: Banco de la Provincia de Córdoba S.A.

El banco de la Provincia de Córdoba S.A. ofrece una amplia gama de servicios financieros. Cuenta con más de ciento cincuenta sucursales ubicadas alrededor de la provincia de Córdoba, una sucursal en Buenos Aires y otra en Rosario. Es una de las principales instituciones financieras del país.

Desafío:

Los directores del Banco de la Provincia de Córdoba están constantemente de viaje, y no tenían acceso al correo electrónico ni cualquier otra forma de recibir documentos que debían revisar y aprobar. Esto retrasaba las respuestas y decisiones de los directores, lo que reducía la eficiencia en las operaciones del banco.

La empresa notó que la interacción del personal entre los diferentes departamentos era limitada, especialmente de aquellos empleados que pasan más tiempo fuera de la oficina, entre ellos los técnicos de TI, representantes de ventas, auditores, supervisores de las sucursales, administradores de riesgo y fraude. Por lo tanto, la productividad se afectaba. También era importante garantizar que el intercambio de información bancaria se hiciera de la forma más segura posible.

Los técnicos de TI tenían que reportar sobre los proyectos de remodelación de las sucursales del banco. Pero sin acceso al correo electrónico o a la información de los proveedores, era difícil informar rápidamente sobre temas, tales como retrasos en la construcción. Además, el personal de TI no podía monitorear la operación de la red del banco estando fuera de la oficina para asegurarse que las transacciones sean procesadas sin interrupciones. Por su parte, los gerentes de ventas también se veían obstaculizados en poder negociar acuerdos con los clientes porque no tenían información clave a mano.[73]

[73] Consultas en Internet: www.ar.blackberry.com/content/dam/blackBerry/pdf/caseStudy/latinAmerica/BancoCordoba_SPA.pdf, (28/10/2013).

Solución:

Para facilitar las tareas diarias sin tener que estar en la oficina, y gracias a la iniciativa del Director Ejecutivo, la empresa equipó a sus altos directores con teléfonos inteligentes BlackBerry, para darles acceso móvil al correo electrónico, contactos, calendarios y otras herramientas. Los empleados del banco también utilizan BlackBerry *Messenger* (BBM) para permanecer en constante contacto con sus colegas, supervisores y proveedores.[74]

Cada sucursal bancaria obtuvo un teléfono inteligente BlackBerry para que los gerentes accedan a la intranet del banco desde el dispositivo, y puedan ver las noticias e informes financieros.

Según el Departamento de Servicio de Comunicaciones Personales de la Gerencia de Tecnología del Banco de la Provincia de Córdoba, se necesitaba una solución que permita a los directores y empleados llevar a cabo sus tareas cotidianas desde sus teléfonos inteligentes BlackBerry, como si estuvieran usando sus propias computadoras de la oficina.

Al reconocer las ventajas de los teléfonos inteligentes BlackBerry, el banco agregó más usuarios de otros departamentos, incluyendo ventas, banca corporativa, auditoría, y administración de riesgo.

Los técnicos de TI que trabajaban en la remodelación de las sucursales del banco utilizaron la cámara de fotos del teléfono inteligente BlackBerry para documentar e informar sobre los avances de la construcción.

El personal de TI también utiliza la aplicación *WhatsUp Gold Mobile Access de Ipswitch Inc*. para supervisar los sistemas de red del banco desde sus teléfonos inteligentes BlackBerry y poder responder rápidamente en caso que surjan problemas en la red.

---

[74] Ibidem.

Para proteger la información en caso de que un teléfono inteligente BlackBerry se pierda o sea robado, el banco utiliza las funciones de administración incorporadas en la solución BlackBerry para borrar los datos de forma remota y restringir el acceso al sistema operativo del banco.

La empresa está en la fase piloto para implementar la aplicación Cortado, creada por el Miembro *Select* de la Alianza BlackBerry, *ThinPrint*, que permite a los usuarios ver, modificar e imprimir documentos que se encuentran en el sistema operativo del banco desde sus teléfonos inteligentes BlackBerry.

Beneficios del Banco:

Al tener acceso a importante documentación remotamente, los directores pudieron supervisar las operaciones, tales como las de mercados financieros y actividades de las cuentas de los clientes. Esto les ayudó a tomar decisiones más informadas cuando están fuera de la oficina, limitando los retrasos y mejorando la productividad.

La solución BlackBerry también permitió que el equipo de ventas cierre acuerdos más rápido, ya que pueden acceder a la información de productos y de precios mientras están negociando con los clientes.

En el proyecto de remodelación de las sucursales del banco, los supervisores en la sede del banco pudieron seguir el progreso de la construcción casi al instante, lo que les permitía resolver rápidamente cualquier problema.

El personal de TI puede trabajar en cualquier interrupción de la red casi de inmediato, prácticamente en todo momento y mientras están fuera de la oficina, desde los teléfonos inteligentes BlackBerry, lo cual es importante para las operaciones diarias del banco.

Debido a su éxito actual, el banco está implementando la aplicación Cortado para que los gerentes de las sucursales puedan enviar los archivos con las transacciones bancarias de cierre y apertura del día desde sus teléfonos inteligentes BlackBerry y los transmitirán al sistema central del banco.

El banco también está en el proceso de desarrollar una aplicación que permite a los gerentes de finanzas aprobar transacciones en línea o ingresar datos financieros, desde sus teléfonos inteligentes BlackBerry.

A medida que siguen descubriendo las muchas ventajas del uso de los teléfonos inteligentes BlackBerry, incorporan más aplicaciones y encuentran incluso más usos para la solución BlackBerry.

6. Caso 3: Diarco

Diarco es una empresa de autoservicio mayorista de productos de almacén, golosinas, bebidas, artículos de limpieza, perfumería, fiambrería, bazar, entre otros, que posee presencia en todo el país. Sus clientes son supermercados, minimercados, almacenes de autoservicio, kioscos, perfumerías y farmacias.

Desafío:

Argentina es el segundo país en tamaño de América del Sur, con aproximadamente 2,6 millones de kilómetros cuadrados, por ende, trasladar productos de una zona a otra es costoso y supone un enorme desafío para compañías como Diarco.

Diarco cuenta en Argentina con 28 sucursales y una fuerza de venta integrada por más de 70 vendedores que efectúan toma de pedidos en más de 50.000 puntos de venta a lo largo y ancho de todo el país. Esta fuerza de ventas realiza operaciones en todo el territorio nacional.

La fuerza de ventas de Diarco, sobre todo la que atendía a clientes del interior del país, situados en localidades muy remotas, tenía algunos inconvenientes en su metodología de trabajo. El vendedor tomaba el pedido a mano y luego enviaba esa hoja por fax a la sucursal de Diarco de donde se abastecía al cliente, allí una persona se encargaba de cargar manualmente el pedido al sistema de Diarco, para posteriormente proceder a prepararlo y despacharlo. Esta metodología contaba con diversos problemas:

- Errores de escritura por parte del vendedor
- Errores de transcripción por parte del personal que cargaba la información
- Largo tiempo de espera entre la toma de pedido, entrega y facturación
- Desconocimiento del estado real de stock al momento de efectuarse la toma de cada pedido

A menudo, el cliente pedía productos que luego no se le entregaban porque el representante de ventas no tenía información del inventario a mano. Esta situación no sólo generaba fricciones con los clientes sino importantes pérdidas en las ventas e inconvenientes en la conciliación de las cuentas por cobrar y cuentas por pagar de los clientes. Para resolver estos problemas, Diarco comenzó a evaluar la posibilidad de que su fuerza de ventas pudiera realizar la toma de pedidos en línea, de sus más de quince mil productos desde cualquiera de los más de cincuenta mil puntos de venta en todo el país, desde un BlackBerry *Smartphone*.[75]

---

[75] Consultas en Internet: www.casosblackberry.com/es/archivos/esp/Diarco_Spanish_BCS_Final.pdf, (26/10/2013).

Solución:

Se otorgaron BlackBerry smartphones a los vendedores con una aplicación desarrollada por Insomnia, miembro de la Alianza BlackBerry. La solución permitió que estuvieran comunicados en todo momento con Diarco y accedieran a la aplicación de toma de pedidos y verificación de inventario.

Algunos aspectos por los cuales Diarco optó por un desarrollo de la solución BlackBerry fueron:

- La facilidad de uso y de capacitación de la fuerza de ventas.
- La comodidad al salir a visitar a los clientes.
- La integración imperceptible del *hardware* (equipo) y del *software*
- La posibilidad de tener un abono plano para los e-*mails*.
- La cualidad de los equipos de poseer un teclado completo, lo cual los hace ideales para la toma de pedidos.
- La seguridad del entorno BlackBerry en el manejo de datos.
- La posibilidad de administrar los dispositivos en forma centralizada para controlar que los usuarios no los utilicen en forma indebida (jugar, sacar fotos, navegar en internet, etc.), logrando así un mejor enfoque de los empleados en los asuntos en los asuntos de la empresa.

La solución de software desarrollada por Insomnia posee un menú de fácil acceso y una interfaz sencilla de uso. Esto permite a los vendedores de Diarco interactuar con una base de datos de más de quince mil produc-

tos, habilitando búsquedas simples y flexibles por código, marca y nombre del producto.[76]

Beneficios de Diarco:

Entre los beneficios alcanzados por Diarco, se destacan los siguientes:

- Asignación de tareas más productivas al personal que ingresaba los datos de forma manual
- Mejora del despacho de órdenes y disminución de errores en los pedidos
- Mejora de la imagen y el servicio al cliente: la nueva tecnología realmente seduce a los clientes y la entrega del producto es mucho más rápida
- Eliminación del envío de fax: El vendedor elimina de su proceso de trabajo el envío de aproximadamente doscientas hojas de fax por día, por vendedor y realiza las gestiones vía *e-mail* en su BlackBerry *Smartphone* casi en el momento en que se produce la venta.
- Reducción de tiempos de entrega y facturación: Diarco recibe los pedidos en el mismo momento en que los toma el vendedor, cargándolos directamente al sistema de la empresa.
- Asignación de tareas más productivas al personal que ingresaba los datos en forma manual: Diarco tenía un gran número de empleados dedicados a cargar en el sistema de la empresa los pedidos que enviaban los vendedores vía fax.

[76] Ibidem.

7. Caso 4: Ministerio de Desarrollo Social

El Ministerio de Desarrollo Social de Argentina es un organismo gubernamental de aproximadamente veinte mil empleados que tiene como objetivos brindar ayuda humanitaria y mejorar las condiciones de vida en comunidades de todo el país. Una gran parte del personal viaja de comunidad en comunidad para reunir información sobre sus necesidades de alimentación y atención médica y sobre la capacidad de respuesta en casos de crisis y desastres naturales.

Desafío:

La velocidad de respuesta y la simplificación de procesos son factores clave para mejorar el flujo de trabajo de cualquier organización. En este caso, hablamos de un organismo que brinda servicios de asistencia social, ayuda en emergencias, educación y apoyo a emprendedores, así que la velocidad de respuesta es crucial.

Como muchas de las comunidades a las que viajan se encuentran en lugares remotos sin acceso a la tecnología, los operadores debían tomar notas a mano y enviarlas por correo tradicional al Ministerio en Buenos Aires. Con esa metodología, obtener una respuesta rápida era casi imposible, ya que las oficinas centrales tardaban por lo menos una semana en recibir la información y las notas tomadas a mano eran poco legibles.[77]

Otra importante labor realizada por el Ministerio es impartir talleres de educación básica y trabajo en zonas remotas. Para eso, los educadores

[77] Consultas en Internet: www.conexionblackberry.com/biz/6122, (24/10/2013).

debían llevar proyectores, computadoras y cámaras, equipos que son caros y frágiles.

Claramente, era necesario optimizar el flujo de trabajo. Para eso, el Ministerio acudió a BlackBerry.

Solución:

El Ministerio equipó a cuatrocientos operadores remotos y otros empleados con *Smartphones* y *tablets* BlackBerry *PlayBook*. Ahora, el proceso es más rápido y fluido.

A la hora de definir un plan de desarrollo social, los trabajadores móviles viajan a las comunidades y llevan en sus dispositivos BlackBerry formularios personalizados. Además de ingresar datos, toman fotografías con la cámara incorporada y adjuntan información geográfica usando las coordenadas obtenidas con el GPS de sus *Smartphones* o *tablets* BlackBerry. Luego, sincronizan el formulario y envían los datos al sistema interno del Ministerio.

De esta manera, los funcionarios tienen una visión integral y pueden acceder rápidamente a la información obtenida para evaluar las condiciones de cada comunidad, aprobar la ayuda que sea necesaria y diseñar programas de asistencia.

Asimismo, los trabajadores de campo utilizan los *tablets* BlackBerry *PlayBook* para dar talleres de capacitación, como la campaña “Argentina Trabaja, Enseña y Aprende”, cuyo objetivo es brindar educación vocacional para adultos. Además, el Ministerio utiliza los *tablets* BlackBerry para capacitar al personal. Al contar con herramientas audiovisuales, los empleados pueden acceder a materiales que les ayudan a comprender y evaluar mejor las necesidades de las comunidades y definir una estrategia de trabajo. El

último paso es poner en marcha un programa de asistencia social personalizado.[78]

El Ministerio también adoptó BlackBerry *Enterprise Server*, por su versatilidad y por las características de seguridad que ofrece. Con esta solución, los empleados tienen acceso rápido, seguro e ininterrumpido a los servidores centrales, estén donde estén, y pueden compartir archivos, fotos y videos de gran tamaño para ayudar a la comunidad.

Beneficios del Ministerio:

La solución BlackBerry permitió optimizar el flujo de trabajo interno y la velocidad de respuesta del Ministerio. Estos son algunos de los beneficios más importantes:

- Tiempos de respuesta más rápidos: Con los *Smartphones* BlackBerry, los funcionarios tienen acceso a información crucial en minutos en vez de semanas. Además, se producen menos errores humanos y el Ministerio cuenta con información más precisa, ya que los empleados completan los formularios directamente en los dispositivos móviles. Esto agiliza la toma de decisiones, que, a su vez, permite aprobar más rápido la compra de alimentos y el desarrollo de programas sociales.

- Tecnología portátil para los trabajadores de campo: Como el Ministerio reemplazó proyectores, computadoras y cámaras por dispositivos BlackBerry compactos y fáciles de llevar, el personal se mueve con mayor facilidad y rapidez.

---

[78] Ibidem.

- Mejoras en los programas de capacitación y educación para comunidades remotas: Ahora, los trabajadores de campo pueden desarrollar programas educativos en comunidades que no tienen electricidad.

- Mejor comunicación con el público: La solución se integra con el sitio web del Ministerio para brindar información al público sobre el estado y el progreso de los programas desarrollados. Esto provee un mayor nivel de transparencia y mejora la precisión de los censos realizados en comunidades lejanas.

CONCLUSIÓN

Cada vez son más las empresas y empresarios independientes que utilizan los *Smartphones* en sus actividades laborales, hacen uso de Internet y suben información a nubes tanto públicas como privadas.

La revolución tecnológica que nos toca vivir produce cambios profundos en las formas de generar, almacenar y compartir información relevante. Dado que los procesos de toma de decisiones cada vez son más cortos, contar con la información oportuna en el momento oportuno es vital para las empresas, y el uso de los teléfonos inteligentes hace una gran contribución en este aspecto.

Para mantener segura la información que se maneja, es fundamental tener en cuenta las consideraciones expuestas, haciendo uso de las herramientas de protección, aplicando las recomendaciones para usuarios y siguiendo las prácticas de seguridad de la información que mejor se adapten al negocio.

Para ejemplificar la aplicación de las consideraciones mencionadas, resulta interesante analizar casos exitosos de soluciones empresariales basados en *Smartphones*, como las implementadas por BlackBerry para sus clientes. De esta forma, resulta fácil apreciar que la solución a grandes problemas puede ser tan pequeña como para caber en la palma de la mano.

ÍNDICE BIBLIOGRÁFICO

a) General:

AGUILERA LOPEZ, Purificación y MORANTE FERNANDEZ, María, Informática 4° ESO, Editorial Cúspide, (México, 2008).

AGUILERA LOPEZ, Purificación, Seguridad Informática, 1° Edición, Editorial Editex S.A., (Madrid, 2010).

CIERCO, David, Cloud Computing: Retos y Oportunidades, (Madrid, febrero de 2011).

DE PABLOS HEREDERO, Carmen, LÓPEZ HERMOSO, José Joaquín, ROMO ROMERO, Santiago Martín, MEDINA SALGADO, Sonia, Organización y transformación de los Sistemas de Información en la Empresa, (Madrid, 2011).

LAUDON, Kenneth C y LAUDON, Jane Price, Sistemas de Información Gerencial, trad. por Antonio Núñez Ramos, 10° Edición, Editorial Pearson Educación, (Nueva York, s.f.).

MORA PÉREZ, José Juan, *Capacity Planning* IT: Una aproximación práctica, (Madrid, 2012).

O´BRIEN, James A y MARAKAS, George M, Sistemas de Información Gerencial, 7° Edición, Editorial Mc Graw-Hill, trad. por María Jesús Herrero Díaz, (México, 2006).

QUERO CATALINAS, Enrique y GARCIA, Román Agustín, Mantenimiento de Portales de la Información, Editorial Paraninfo, (España, 2007).

ROIG, Oriol Salent y VALENZUELA GONZALEZ, José Luis, Principios de Comunicaciones Móviles, 1° Edición, Editorial Cuspide, (Cataluña, 2003).

b) Especial:

JOYANES AGUILAR, Luis, Computación en la Nube - Estrategias de Cloud Computing en las empresas, Editorial Alfaomega, (México, 2012).

TORRES VIÑALS, Jordi, Empresas en la Nube. Ventajas y Retos del Cloud Computing, Editorial Libros de Cabecera, (España, 2012).

URUEÑA, Alberto, El Estudio Cloud Computing. Retos y Oportunidades, (España, Mayo de 2012).

c) Otras publicaciones:

Consultas en internet: www.altonivel.com.mx, (10/10/2013).
_____ www.aprenderinternet.about.com, (01/09/2013).
_____ www.archivos.usuaria.org.ar, (26/09/2013).
_____ www.areatecnologia.com, (05/10/2013).
_____ www.atc.ugr.es, (20/10/2013).
_____ www.audienciaelectronica.net, (11/10/2013).
_____ www.avg.com, (15/10/2013).
_____ www.blackberry.com, (22/10/2013).
_____ www.blog.kaspersky.es, (30/10/2013).
_____ www.blog.segu-info.com.ar, (15/10/2013).
_____ www.casosblackberry.com, (26/10/2013).
_____ www.cisco.com, (22/09/2013).
_____ www.conexionblackberry.com, (24/10/2013).
_____ www.csirtcv.gva.es, (02/10/2013).
_____ www.eficienciagerencial.com, (24/09/2013).
_____ www.entel.cl, (30/09/2013).
_____ www.eset_la.com, (08/10/2013).

_____ www.espaciocloud.com.ar, (23/10/2013).
_____ www.everis.com, (12/09/2013).
_____ www.feederico.com, (29/07/2013).
_____ www.informatica-hoy.com.ar, (10/10/2013).
_____ www.inteco.es, (18/09/2013).
_____ www.iprofesional.com, (15/10/2013).
_____ www.iso27000.es, (28/09/2013).
_____ www.itsmf-argentina.org.ar, (02/09/2013).
_____ www.kaspersky.com, (28/10/2013).
_____ www.lema.rae.es, (15/10/2013).
_____ www.navactica.com, (05/10/2013).
_____ www.ontsi.red.es, (25/08/2013).
_____ www.pcworld.com.mx, (28/10/2013).
_____ www.redseguridad.com, (10/09/2013).
_____ www.sahw.com, (26/08/2013).
_____ www.securitinghuman.org, (07/09/2013).
_____ www.seginfo.tripod.com, (03/09/2013).
_____ www.seguridadparatodos.es, (30/08/2013).
_____ www.skype.com, (15/10/2013).
_____ www.telcommunity.com, (12/10/2013).
_____ www.thinprint.com, (14/09/2013).
_____ www.tuexperto.com, (30/08/2013).
_____ www.viruslist.com, (18/10/2013).
_____ www.whatsapp.com, (10/10/2013).
_____ www.wikipedia.org, (29/08/2013).
_____ www.zma.com.ar, (03/10/2013).

KASPERSKY LAB, Los Retos de la Seguridad Móvil en el Entorno Corporativo, Artículo técnico, (Madrid, 2012).

ÍNDICE

Pág.

Abstract.....…… 1

Prólogo.....…… 2

CAPÍTULO I

Tecnologías de Información

1. Las tecnologías de información en las empresas..…….. 3

2. ¿Qué es un *Smartphone*?..... 6

3. Prestaciones del *Smartphone*…….. 7

4. Ventajas de los *Smartphones*……... 8

5. Desventajas de los *Smartphones*…… 10

CAPÍTULO II

Sistemas Operativos y Aplicaciones en los Smartphones

1. Sistemas operativos móviles……. 12

2. Android……. 13

3. iOS…… 14

4. Blackberry OS…… 15

5. Windows Phone……. 16

6. Aplicaciones para Smartphones…….……..... 17

CAPÍTULO III

Cómo se transmiten los datos en los Smartphones

1. Red Inalámbrica……. 22

2. Wi-Fi……. 24

3. Bluetooth……. 25

4. GSM…… 27

5. GPRS…… 28

6. Conexión EDGE…… 29

7. Conexión 3G…….. 31

8. Conexión 4G…… 32

CAPÍTULO IV

Peligros Expuestos en los Smartphones

1. Vulnerabilidad de los sistemas…….. 34

2. Vulnerabilidad de Internet y los servicios inalámbricos…….. 36

3. Definición y clasificación de los *Hackers*…….. 38

4. *Software* malicioso de los *Smartphones* 41

5. Peligros latentes de los *Smartphones*. 48

CAPÍTULO V

La Seguridad en los Smartphones

1. Seguridad Informática…… 52

2. Seguridad en los Smartphones en entornos corporativos…… 54

3. Software de protección frente al robo y la pérdida……. 56

4. Cifrado o encriptado del dispositivo……. 57

5. Reconocimiento biométrico…….. 59

6. Copias de Seguridad……. 60

7. Protección Antivirus…….. 62

8. Otras recomendaciones para usuarios…… 63

CAPÍTULO VI

Buenas Prácticas para la Seguridad de la Información

1. Origen de la ISO 27000…… 66

2. La Serie 27000…….. 68

3. ISO 27002: Buenas Prácticas para la Seguridad de la Información.. 74

4. Gestión de Operaciones y Comunicaciones……. 76

5. Control de Accesos…… 81

CAPITULO VII
Cloud Computing

1. Origen del Cloud Computing……. 93

2. Concepto de Cloud Computing…… 95

3. Características del Cloud Computing…..…….. 98

4. Ventajas del Cloud Computing……. 103

5. Desventajas y Riesgos del Cloud Computing……. 109

6. Seguridad y Privacidad de los Datos…… 112

CAPÍTULO VIII
BlackBerry – Casos Exitosos de Aplicación

1. El concepto de Seguridad para BlackBerry…… 116

2. Principales Productos y Servicios Empresariales…….. 118

3. Prestaciones para Empresas……. 126

4. Caso 1: Cablevisión S.A…… 131

5. Caso 2: Banco de la Provincia de Córdoba S.A……. 134

6. Caso 3: Diarco…… 138

7. Caso 4: Ministerio de Desarrollo Social…….. 142

Conclusión…… 146

Índice Bibliográfico…… 147

Índice…… 150