AndalucíaCERT
CENTRO DE SEGURIDAD TIC

Informe de divulgación
Seguridad en movilidad

Tipo de documento:	*Informe*
Autor del documento:	*AndalucíaCERT*
Código del Documento:	*CERT-IF-1230-111111*
Edición:	*0*
Categoría	*Público*
Fecha de elaboración:	*11/11/2011*
N° de Páginas	*1 de 13*

1 TABLA DE CONTENIDOS

2 OBJETO

El objeto de este documento es proporcionar al personal de la Junta de Andalucía una guía de buenas prácticas en el uso de las distintas soluciones de movilidad existentes actualmente.

3 ALCANCE

El documento va destinado al personal de la Junta de Andalucía y público en general.

4 LA ERA DE LA CONECTIVIDAD

La movilidad en las nuevas tecnologías está cambiando nuestras vidas, en la conferencia D8 el recientemente fallecido y ex-CEO de Apple Steve Jobs se refirió al estado actual y futuro de los ordenadores personales: *"Se acerca el día en que muy pocas personas, en casos aislados, necesitarán un ordenador tradicional. Cuando éramos un país agrícola todos los vehículos eran tractores, porque era el tipo vehículo que se necesitaba en las granjas"*. Jobs comparó los PCs con los tractores, afirmando que, aunque van a seguir existiendo, *"sólo una de cada x personas los necesitarán".*

Actualmente, la movilidad es ya una realidad que está modificando nuestras vidas en todos los ámbitos. Como todos los grandes cambios, la movilidad proporciona grandes ventajas y oportunidades; sin embargo, presenta también grandes retos que han de ser superados.

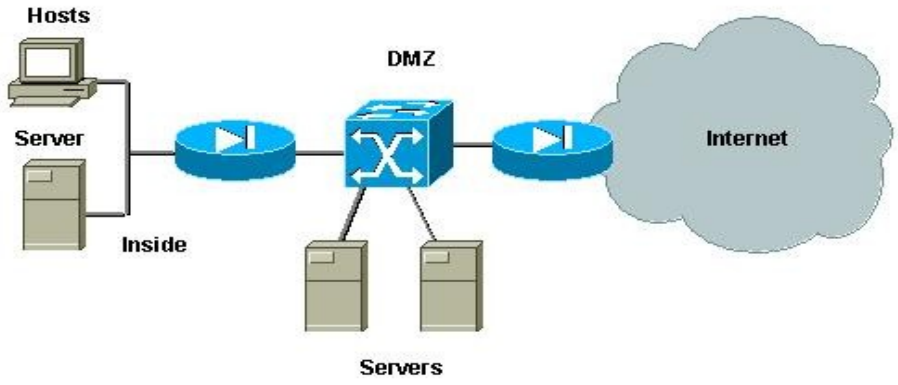
Internet ha impulsado grandes cambios en la forma de comunicarnos, el aumento en las velocidades de conexión, el abaratamiento de los costes de conexión, de los terminales y dispositivos, han permitido un acceso masivo a Internet, tanto a usuarios particulares como a empresas, estas últimas han hecho de la red una necesidad fundamental para llevar a cabo sus negocios y aumentar la productividad de sus empleados. La **era de la conectividad** ha supuesto un cambio en el diseño y uso de las redes corporativas: Usuarios conectados 24 horas al día, desde distintas partes del mundo a través de diversos dispositivos: netbooks, portátiles, smartphones, tablets... Lo que anteriormente eran usuarios conectados en espacios de trabajo estáticos, ahora son usuarios móviles utilizando servicios y dispositivos para mantenerse conectados con la red corporativa y los recursos necesarios.

Sin embargo, el aumento de la productividad asociado al aumento de la movilidad de los empleados no es gratuito, el **equilibrio entre movilidad y seguridad** debe ser clave para las organizaciones. Los usuarios cada vez tienen terminales móviles con mayores prestaciones y ven necesario usarlos para acceder a datos o aplicaciones para realizar su trabajo. La libre circulación del usuario plantea una serie de amenazas que deben ser consideradas a la hora de diseñar una política de seguridad, comenzando por concienciar al usuario de la problemática que genera la ausencia de barreras físicas. Por ello: ¿cuáles son los riesgos para la seguridad de la información en la era de la conectividad? ¿existe una adecuada cultura de seguridad organizativa al respecto?

El objetivo de este documento es analizar los diversos componentes que deben ser protegidos por la organización en las diferentes soluciones de movilidad, describir los principales riesgos que afectan a cada uno de ellos y presentar una serie de recomendaciones para los usuarios finales y administradores de sistemas.

5 LA AMPLIACIÓN DEL PERÍMETRO

Hasta hace poco, el esquema de una red corporativa se basaba en la implementación de una manera más o menos compleja del concepto de perímetro: Un límite virtual entre la red interna e Internet, delimitado generalmente por una serie de componentes como routers o firewalls: todas las comunicaciones que provengan desde Internet hacia la organización, o que salgan desde la organización hacia otras redes, deben pasar por el perímetro. Una de las principales funciones del perímetro es verificar si cada dato que pasa a través de él es correcto y seguro, en el caso de que no sea así, es detenido, asimismo, es posible implementar medidas de seguridad en dicho perímetro, como pueden ser la prevención de ataques externos, control del correo electrónico no deseado o la prohibición de acceso a sitios web no permitidos.



Resumiendo, la definición de un perímetro nos permite delimitar qué se encuentra dentro de la organización y qué se encuentra fuera, por otra parte, también nos permite coordinar de una manera más o menos centralizada las políticas de acceso hacia o desde la organización.

Sin embargo este concepto en la actualidad es tan sencillo como obsoleto. La era de la conectividad ha traido como consecuencia **una serie de componentes que modifican esa estructura de red clásica**, que hasta hace unos pocos años era eficiente en lo que respecta a seguridad.

Supongamos el caso de un responsable de área que va a una conferencia a Norteamérica con un portátil de empresa y su tablet PC personal. Mediante ambas se conectará a varias redes Wi-Fi (aeropuerto, hotel, sala de conferencias, en empresas colaboradoras, etc...), se descargará el correo electrónico de la organización, sincronizará los archivos de sus distintas cuentas en los dispositivos, conectará dispositivos USB ajenos e incluso es posible que otros utilicen el ordenador. Posteriormente el responsable de área regresa al espacio físico de la organización y conecta su portátil a la red corporativa.

¿Dónde está el perímetro que controla si la información puede o no ser utilizada? ¿En la empresa? ¿En Norteamérica?

Como vemos, el viejo concepto de perímetro, queda obsoleto. El perímetro en las redes corporativas actuales es, cuanto menos difuso, y eso implica a una serie de amenazas y riesgos que deben ser entendidos.

6 EL HARDWARE Y LOS DISPOSITIVOS

Hasta hace poco, la mayoría del hardware que contenía información importante para una organización se encontraba inventariado y a buen recaudo. Si las políticas de seguridad se encontraban correctamente implementadas, desde un puesto de escritorio estático era difícil que se produjera una fuga importante de información, por otra parte, debido a motivos obvios de portabilidad, también era difícil que alguien pudiera introducir un dispositivo dentro de la red de la organización sin levantar sospechas.

En la actualidad el tamaño de los dispositivos se ha reducido enormemente tanto en ordenadores portátiles o netbooks como los teléfonos de nueva generación o discos portátiles USB, este hecho unido al aumento de la capacidad de almacenamiento en dichos dispositivos, hace que sea posible trasportar una gran cantidad de datos de una manera muy cómoda. Sin embargo, esto implica que la cantidad de datos que potencialmente pueden verse comprometidos en caso de pérdida o robo de cualquiera de estos dispositivos tanto de índole personal (fotos, mensajes, mails privados...) como corporativos (documentos, planes de negocio, facturas, datos de clientes...) es lo suficientemente importante como para estudiar tomar ciertas medidas.

Ademas de lo anterior, hay que contar con las distintas cuentas en servicios online que habitualmente son accesibles por defecto en smartphones y tablets PC (correo, cuenta de Facebook, Twitter...) Piense. ¿Qué ocurriría si pierde o le roban su teléfono móvil? ¿Cuántos contactos perdería? ¿A qué información podría acceder quien tuviera el control del dispositivo?

En el caso de empresas y organizaciones permitir la introducción de elementos extraños en la red corporativa conlleva una serie de riesgos que deben ser tenidos en cuenta a la hora de establecer una política de seguridad. Debido a los distintos dispositivos usados por los integrantes de la organización, es posible trasportar información (potencialmente sensible) desde y hacia ésta. Estos usuarios móviles utilizan la información no sólo cuando están dentro de la red corporativa, sino también en otros ámbitos como su hogar, otras organizaciones o redes, o incluso en movimiento. Entonces, ¿cómo diferenciamos un usuario doméstico o particular de un usuario de una red corporativa?

Otra de la característica de la era de la conectividad es la velocidad el crecimiento de la dependencia y el aumento del consumo de la tecnología de la información. Esto, unido a la necesidad de las empresas de reducir costes, a la discordancias entre las directivas de las organizaciones y a los avances en las capacidades de trabajo de los dispositivos móviles, hace que una gran cantidad de usuarios domésticos utilicen sus dispositivos también para actividades profesionales o viceversa, por lo que línea

que separa el antiguo concepto de equipo de trabajo y de ocio se torna difusa, además, este hecho implica una serie de riesgos que habitualmente son desconocidos para el usuario.

Es por ello que las recomendaciones que aquí vamos a exponer son válidas tanto para usuarios particulares como para aquellos que pertenezcan a alguna organización. Vamos a presentar a continuación los dispositivos más comunes que presentan las características típicas de uso en movilidad, enumeraremos los riesgos y realizaremos recomendaciones para mitigar las amenazas de seguridad.

6.1 Dispositivos USB

Esta categoría engloba a todo tipo de memorias con conector USB: Pendrives, discos duros externos, cámaras de fotos, reproductores de música...
Dichos dispositivos permiten a los usuarios llevar y traer información a la red de la organización, pero que a la vez son conectados en ordenadores que no poseen las medidas de seguridad que se utilizan dentro de la red, es por ello que este tipo de dispositivos se encuentran muy expuestos a infecciones por distintos tipos de códigos maliciosos, lo cual supone un riesgo para la seguridad de la organización.

Riesgos:

- Pérdida del dispositivo.
- Robo.
- Infección por algún tipo de código malicioso.
- Fuga de información.

Recomendaciones:

- Cifrado del dispositivo: Lo cual evitaría su lectura en caso de extravío o robo del dispositivo.
- Establecer políticas de seguridad claras con respecto al uso de dispositivos extraíbles y que los usuarios conozcan y respeten estas políticas.
- Limitar el acceso a estos dispositivos y registrar el uso de los mismos.
- En casos extremos se puede bloquear, por medio de políticas de grupo, de dominio o corporativas, el uso de estos dispositivos.
- Ya sea en el hogar o en las organizaciones, revisar con un antivirus con capacidades proactivas cualquier dispositivo que se conecte al equipo.
- Desactivar el arranque automático de los dispositivos extraíbles.

6.2 Portátiles y Netbooks

Los ordenadores portátiles permiten no sólo transportar información hacia fuera del perímetro, sino también la alteración de la misma, además nos permite acceder a otras redes con diferentes (o inexistentes) medidas de seguridad, que pueden presentar vulnerabilidades o ataques que tengan como objetivo la información corporativa que resida dentro del perímetro.

Riesgos:

- Robo.
- Avería de alguno de los componentes del equipo con la consiguiente imposibilidad de acceso a los datos.
- Pérdida del equipo y de los datos que contiene.
- Acceso no deseado al equipo.
- Robo de identidad corporativa o personal: Mediante contraseñas guardadas o accesos a la VPN de la organización.
- Posibilidad de encontrarse infectado por algún tipo de código malicioso, con el consiguiente peligro para la red de la organización.

Recomendaciones:

- Cifrado de los distintos datos del equipo.
- Realización periódicas de copias de seguridad de los datos del equipo.
- Proteger el acceso al sistema operativo y a la BIOS mediante contraseñas.
- Mantener el equipo bajo vigilancia.
- Tener el equipo identificado: anotar sus datos distintivos (marca, modelo, número de serie..).
- Usar medidas biométricas de acceso, si el equipo lo permite.
- Implementación de sistemas antirrobo físicos (candados, sistemas de anclado).
- Configure su equipo para que se bloquee automáticamente transcurrido un determinado período de tiempo.
- Contar con el software de seguridad necesario (Antivirus, Firewall, etc..).

6.3 Smartphones/Tablets PC

Un teléfono de última generación o un tablet poseen funcionalidades similares a los ordenadores portátiles, a las que se suman particularidades específicas de este tipo de dispositivos, la alta capacidad para conexión en redes inalámbricas (wireless, bluetooth, Internet) y la mayor facilidad con la que este tipo de dispositivos puede ser perdido o robado.

Como hemos indicado en puntos anteriores, un hecho que cada vez se da con más frecuencia es el uso por parte de los empleados que utilizan sus dispositivos personales en el trabajo, esto es debido a diferentes motivos:

- El terminal ofrecido por la organización es de mayor prestación que el usado por el empleado.
- La necesidad de las empresas por reducir costes hace que se permita al usuario usar su dispositivo personal como terminal de trabajo.
- La motivación del mismo usuarios por elegir su propio dispositivo.

El uso un mismo dispositivo como equipo de trabajo y de ocio,a pesar de las ventajas inherentes en cuanto a comodidad, ocasiona un evidente riesgo de seguridad ya que aumenta la probabilidad de pérdida o robo y dobla la cantidad de datos que pueden ser expuestos en este caso.

Riesgos:

- Robo.
- Pérdida del dispositivo.
- Fuga de datos confidenciales/personales.
- Robo de identidad del usuario corporativo/personal.

Recomendaciones:

- Uso de aplicaciones para el seguimiento del dispositivo mediante GPS: Existe aplicaciones que permiten incluso el bloqueo o el borrado remoto de los datos del dispositivo.
- Infórmese sobre las amenazas contra los dispositivos móviles. En general, son similares a las que circulan en el mundo online. Puede sufrir ataques de hackers, de virus o de phishing en su dispositivo móvil del mismo modo que cuando navega por Internet.
- Realice copias de seguridad frecuentes de sus datos.
- Configure su dispositivo para que se bloquee automáticamente transcurrido un determinado período de tiempo.
- No almacene datos que no puede permitirse perder.
- Familiarícese con la directiva sobre dispositivos móviles de su organización y sobre sus objetivos, y considere si satisface sus necesidades. Si es así, acéptela; en caso contrario, utilice dos dispositivos: uno para uso personal y otro para su actividad profesional.
- Minimice el número de servicios online accesibles sin contraseñas por defecto.
- No mantener el equipo sin vigilancia.
- Tener el equipo identificado: anotar sus datos distintivos (marca, modelo, número de serie..).

7 NUEVAS TECNOLOGÍAS Y AMENAZAS PARA LOS USUARIOS EN MOVILIDAD

7.1 Ataques a dispositivos móviles

Con el auge de los smartphones conectados a Internet, debido a que este tipo de dispositivos cada vez tienen un acceso mayor a información sensible (tanto empresarial como privada) y a que normalmente las redes móviles y 3G's no suelen estar contempladas en las acciones preventivas de seguridad de las organizaciones, los cibercriminales han visto un nuevo filón para atacar a los usuarios, mediante diferentes métodos. Las principales amenazas hacia dispositivos móviles que nos encontramos actualmente son:

- *Ataques basados en Web y Redes:* Son lanzados por sitios web maliciosos o sitios ilegitimos que han sido comprometidos. El sitio malicioso que lanza el ataque se aprovecha del browser en el dispositivo e intenta instalar malware o robar datos confidenciales.
- *Malware*: Funcionan de la misma manera que para los ordenadores personales (Gusanos, caballos de troya, botnets...)
- *Ataques de ingeniería social*: Usando redes sociales, spam u otro tipo de comunicaciones. El objetivo es engañar a los usuarios para que revelen datos sensibles o instalen malware. En esta categoría se encuadran los ataques de phishing.

- *Abuso de recursos*: Se busca el uso indebido del dispositivo o los recursos que éste posee: Envío de spam, ataques de denegación de servicio...
- *Pérdida de datos:* Empleado de una organización o ciberdelincuente extrae información sensible del dispositivo o de alguna de las redes que usa. Puede ser intencionada o inintencionadamente
- *Amenazas asociadas a la integridad de los datos:* Su propósito es interrumpir las operaciones de una empresa u obtener ganancias financieras. Puede ocurrir sin intención

Recomendaciones:

- Activar las conexiones Bluetooth, Infrarrojos y Wi-Fi sólo cuando se vayan a utilizar.
- Cuidado con las tarjetas de memoria: Desconfíe de las tarjetas de memoria si tienen una procedencia desconocida o si han sido introducidas en dispositivos no confiables ya que es posible que se encuentren infectadas por algún tipo de malware.
- Desconfíe de las aplicaciones no confiables, extrañas, descargadas de sitios no oficiales o de redes P2P ya que pueden contener malware u otro tipo de amenazas.
- Mensajes SMS o MMS no solicitados. Es posible que recibamos mensajes de texto o bien multimedia de fuentes que desconocemos invitándonos a descargar un archivo o visitar cierta URL. En ningún caso es recomendable seguir estos enlaces si vienen de una fuente desconocida o aluden a un servicio no solicitado.
- Actualizar el firmware y el software del sistema operativo y de las aplicaciones de manera frecuente. Es importante mantener el smartphone al día en cuanto a dichas actualizaciones se refiere, no solo para garantizar un correcto funcionamiento, sino para estar seguros de que tenemos instaladas las últimas actualizaciones de seguridad

7.2 Cloud computing: Nuevas tecnologías, nuevas amenazas

El cloud computing es un modelo a la carta para la asignación y el consumo de computación. Describe el uso de una serie de servicios, aplicaciones, información e infraestructura compuesta por reservas de recursos de computación, redes, información y almacenamiento. Las características son:

- Escalabilidad sobre demanda.
- Infraestructura compartida.
- Independencia de ubicaciones físicas.
- Precio por consumo.
- Aprovisionamiento inmediato.
- Acuerdos de nivel de servicio.
- Alto nivel de disponibilidad.

Como vemos, el cloud computing es un modelo que permite el acceso "on demand" a un conjunto compartido de recursos informáticos, de los cuales se puede disponer rápidamente con una gestión mínima de esfuerzos. Esto permite claras ventajas para los clientes como unos precios más flexibles, actualizaciones de las plataformas de manera automática, servicios disponibles en cualquier lugar y una

mínima cantidad de tiempo fuera de servicio. En definitiva, permite centrarse en el negocio y adoptar menor riesgos a la hora de desarrollar un proyecto.

Sin embargo, esta tecnología también comporta riesgos, los servicios en la nube son una "caja negra" dejándose en manos del proveedor del servicio la responsabilidad del almacenamiento de datos y su control sin considerar legislación, normas ni regulaciones. Por tanto la confidencialidad, la integridad o disponibilidad de los datos pueden verse comprometidas.

Aparte de este hecho, también hay que tener en cuenta otros riesgos desde el punto de vista de la seguridad:

- Usuarios del recurso compartido que pueda acceder a nuestro servicio.
- Se desconocen los activos del proveedor, por tanto no sabemos si los sistemas que usan se encuentran correctamente protegidos o son una amenaza.
- Existe la posibilidad de un ataque por robo de sesión o una suplantación de identidad mediante el acceso a un equipo con los credenciales o mediante el robo de contraseña.

Por todo ello en necesario tomar ciertas medidas para proteger los tres pilares de la seguridad de la información:

Protección de la confidencialidad

- Es necesario verificar dónde se alojan los datos para evitar problemas de legislación y geolocalización.
- Es necesario conocer quién accede a la información almacenada
- El cifrado debe realizarse en la información almacenada, en transito y en backup.
- Se debe verificar si se retiene o se destruye la información al finalizar el contrato con el proveedor.

Protección de la Integridad

- Es necesario analizar quién puede acceder, modificar o eliminar información del centro de datos.
- Verificar si la información permanece o se elimina lógica/físicamente teniendo en cuenta la remanencia.
- Verificar si es posible que los datos de distintos cliente se "mezclen".
- Comprobar si poseen sistemas de análisis de malware.

Protección de la disponibilidad

- Se puede asumir que los servicios no estarán disponibles 24x7, sin embargo los proveedores ofrecen hasta un 99,999% de disponibilidad.
- Es necesario contar con que puedan existir ataques de DDOS.
- Se debe tener presente que es un servicio con un punto de fallo único SPOF (Single Point of Failure).

Por otra parte, ya que no es posible conocer los activos, ni las amenazas (al menos no totalmente) es imposible medir el riesgo ni implementar ningún tipo de control. Por lo tanto es de suma importancia fortalecer las medidas contractuales, estipulando todo lo necesario en los ANS (acuerdos de nivel de servicio) y analizando el sistema de penalizaciones.

8 ¿CÓMO ACTUAR EN CASO DE PÉRDIDA O ROBO DEL DISPOSITIVO?

- Si se trata de un terminal móvil, póngase en contacto con su operador y proceda al bloqueo de la tarjeta SIM para impedir la realización de llamadas con cargo al usuario.
- De la misma manera, bloquee el terminal para su uso en redes, para ello necesitara proporcionar al proveedor el IMEI del dispositivo.
- Solicite el borrado remoto de la información del dispositivo si dispone de este servicio.
- Si procede, curse la correspondiente denuncia ante la autoridad competente. Será necesaria una descripción completa del dispositivo: Marca, modelo, identificador. Si es posible sería recomendable proporcionar una fotografía del equipo.
- Enumere los servicios "en la nube" a los que tenia acceso su dispositivo de manera automática (Cuentas de correo, Redes sociales, etc..) y cambie las contraseñas de acceso.
- Si tenía certificados digitales instalados en el dispositivo, será necesario revocar y solicitarlos de nuevo.
- Si su dispositivo tenía configurado algún tipo de credenciales para el acceso a alguna red privada virtual, póngase en contacto con el administrador del sistema.
- Cambie cualquier tipo de contraseña que pueda haber sido accesible con los datos obtenidos del dispositivo, sobre todo aquella relativa a los accesos de Hosting y Cloud Computing.
- Si ha perdido información importante o sensible, comuníquelo de manera inmediata para poder valorar el impacto.

9 CONCLUSIONES

La dependencia de los dispositivos móviles es ya muy significativa y crece rápidamente en un entorno muy heterogéneo en el que existe mucha libertad de uso. Es necesario empezar a comprender que los dispositivos ya no son exclusivamente de uso particular o profesional, cumplen ambas funciones. Por tanto, la seguridad móvil debe estar integrada en el dispositivo y en la red de manera conjunta.

Como hemos visto a lo largo del documento, las principales dificultades para implementar seguridad en la nueva era de la conectividad son:

- *Dificultad para implementar controles de seguridad:* Con los nuevos componentes de hardware, mucha información corporativa es accedida desde nuevos dispositivos, que incluso pueden ser personales y no pertenecer a la empresa. Por lo tanto, deben definirse nuevos controles de seguridad, contando con el handicap de no poder controlar toda la administración necesaria (computadoras personales, servidores externos, entre otros).

- *Dificultad para mantener la monitorización sobre el hardware*: Los nuevos componentes de hardware "salen y entran" de la red, conectándose de manera temporal. Cuando estos dispositivos están fuera de la red, no es posible monitorizar su uso, estado o los riesgos a los que se expone.
- *Dificultad para establecer controles perimetrales*: Los controles ya no pueden ser clasificados en internos, externos y perimetrales, sino que deben definirse nuevos controles que rompen con el esquema del perímetro. ¿Dónde se deben controlar el correo no deseado? ¿Dónde se deben controlar los accesos no autorizados? ¿Existen dispositivos para ello?
- *Dificultad para controlar quién utiliza los recursos de la organización*: Cuando los recursos de hardware de la organización (esencialmente los dispositivos móviles) son transportados fuera de la red corporativa, no es posible garantizar que sólo serán utilizados por personal de la organización.
- *Dificultad para conocer controles de seguridad al contratar servicios externos*: Al incrementarse el número de proveedores que almacenan información sensible de la organización, se plantea la problemática de no poder intervenir en las políticas de seguridad que éstos poseen sobre sus servicios, y que incidirán directamente sobre la información sensible de la organización

El esquema de seguridad basado en el perímetro ofrecía un marco para definir un entorno controlado (la red corporativa), y otro no controlado. Este entorno ya no es tal, y la era de la conectividad presenta un escenario híbrido donde la información corporativa se almacena y transporta con un dinamismo cada vez mayor.

La pérdida y la filtración de datos son la mayor preocupación tanto para usuarios como para organizaciones, en este último ámbito es patente que existe personal externo, en muchos casos, cambian de trabajo cada pocos años. Cuando ocupan un nuevo puesto, llegan con sus propios dispositivos, pero cuando se van, deben devolver los datos que pertenecen a la organización, así mismo, las organizaciones deben encontrar una forma de facilitar ese proceso, respetando lo que trajo el empleado a la compañía y su privacidad.

Por tanto, la seguridad en movilidad, tal y como se nos plantea, debe transformarse en una combinación cuidada y coordinada de tecnologías modernas en conjunción de dos vertientes: la gestión de la seguridad y la educación de usuario.

Gestión de la seguridad

La gestión de la seguridad debe ser considerada de mayor importancia a lo que se acostumbra en un entorno corporativo. La definición de políticas de seguridad claras permite que los usuarios móviles, ahora transportadores de información, puedan conocer qué está permitido y qué no lo está, con relación a los recursos y la información de la empresa.

Además, como el modelo de la seguridad se vuelve más complejo, es importante contar con herramientas que permitan evaluar y tasar los costos de las medidas de seguridad a implementar, por lo que se hace necesario definir herramientas necesarias para este fin.

Educación del usuario

La manera más eficiente de que las políticas de seguridad sean implementadas como se debe, y las tecnologías de seguridad utilizadas por cada uno de los usuarios, es la concienciación.

Educar a los usuarios permite involucrar a estos en el proceso de proteger los activos de la empresa y para ello la organización debe establecer capacitaciones y programas de educación de manera periódica y regular, adaptadas a las características de la organización y el rol de los empleados.

En resumen, el trabajo conjunto entre tecnologías, gestión y educación dan respuesta a este cambio de paradigma: no sólo se debe proteger la red, se debe proteger al usuario y todo su entorno

10 DOCUMENTACIÓN DE REFERENCIA

- INTECO: Protección del puesto de trabajo: Dispositivos y usuarios. Catálogo de empresas y soluciones de seguridad TIC
- Cloud Security Alliance: Guía para la Seguridad en áreas críticas de atención en Cloud Computing
- Clearswift Protection: Data Leak Protection
- INTECO: Riesgos y amenazas en Cloud Computing
- INTECO: Seguridad en movilidad
- Cristian Borghello: Seguridad en Cloud Computing