Movilidad del usuario: seguridad en la era de la conectividad

Autor: Sebastián Bortnik, Analista en Seguridad de ESET para Latinoamérica
Fecha: viernes 27 de agosto de 2010

ESET Latinoamérica, Av. Del Libertador 6250, 6to piso
Buenos Aires, C1428ARS, Argentina
Tel. +54 (11) 4788 9213 - Fax. +54 (11) 4788 9629
info@eset-la.com, www.eset-la.com

Índice

Introducción **3**

El perímetro, ese viejo amigo de la seguridad **4**

El nuevo escenario **5**

Hardware 5

Conectividad 8

Software 8

Otros riesgos asociados 8

Desafíos y problemáticas **9**

Nuevo escenario de defensa **10**

Tecnologías de seguridad 10

Gestión de la seguridad 11

Educación del usuario 11

Conclusión **11**

Referencias **12**

Introducción

Internet impuso grandes cambios en las formas de comunicación y, en consecuencia, en la infraestructura de las redes corporativas. Los aumentos en las velocidades de conectividad y la utilización de conexiones de banda ancha dieron acceso a Internet a todas las empresas, como necesidad fundamental para llevar a cabo sus negocios.

Luego de la masificación de este tipo conexiones, una nueva era de Internet modifica su uso en las redes corporativas: **la era de la conectividad**. Esta expresión señala a los usuarios conectados las 24 horas del día a Internet, a través de diversos equipos como laptops, *pockets pc*, *smartphones*, y otros. Lo que antes eran individuos conectados en espacios de trabajo estáticos, ahora son usuarios móviles, utilizando tanto hardware como software y servicios para mantenerse conectados en todo tiempo y espacio a las redes y recursos corporativos, utilizando Internet como principal medio para este fin.

Sin embargo, **¿cuáles son los riesgos para la seguridad de la información de la empresa en la era de la conectividad?** La movilidad del usuario genera la ausencia de barreras físicas y expone a la información de la organización a una serie de amenazas, que deben ser consideradas a la hora de diseñar la política de seguridad corporativa.

El objetivo del presente trabajo es analizar los diversos componentes que deben ser protegidos por la organización, además de la propia red interna; se describirán cuáles son los principales riesgos que afectan a cada uno de ellos; y se señalará cuáles son los cambios en la forma en que se abarca la seguridad de la información en un entorno empresarial.

El perímetro, ese viejo amigo de la seguridad

Con la masificación del acceso a Internet, las redes corporativas enfrentaron la obligación de controlar la entrada y salida de información de la empresa hacia el ciberespacio. Un esquema de red corporativa básica suele ser representado de la siguiente manera:

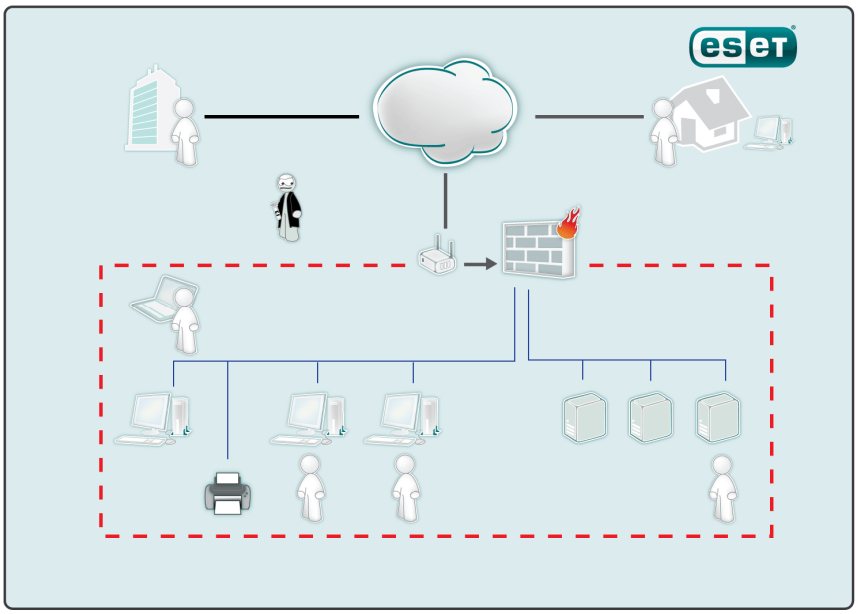


Imagen 1 – Red corporativa con perímetro

En esta imagen se observa en color rojo un componente fundamental del gráfico: **el perímetro**. Se trata de un límite virtual entre la red interna e Internet, delimitado generalmente por una serie de componentes o servidores como *routers* o *firewalls*. El concepto es muy sencillo: todas las comunicaciones que provengan desde Internet hacia la empresa, o que salgan desde la empresa hacia otras redes, deben pasar por el perímetro.

Una de las funciones primordiales del perímetro es la seguridad: cada dato es controlado para verificar si es correcto (y seguro) que el mismo continúe su flujo de información, caso contrario, es detenido. Por ejemplo, en un esquema como el presentado, algunas de las medidas de seguridad que se suelen implementar en el perímetro, entre otras, son la prevención de ataques externos, el control del correo electrónico no deseado o la prohibición de acceso a sitios web no permitidos.

En resumen, el perímetro permite definir claramente qué está adentro de la red corporativa, qué está fuera de la misma, y cuáles son los criterios o políticas de acceso desde y hacia otro sector.

Sin embargo este concepto en la actualidad **es tan sencillo como obsoleto**. La era de la conectividad trajo 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.

Por ejemplo, suponiendo el caso del gerente de una organización que viaja a Europa con una computadora portátil la cual posee información confidencial de la empresa. Con la misma *laptop* se conecta a las redes inalámbricas del hotel y de varios de los clientes que visita en su estadía. Además, conecta a la computadora dispositivos USB de terceros, e incluso otros utilizan esa misma computadora. Posteriormente el mismo gerente vuelve al espacio físico de su empresa.

¿Dónde está el perímetro que controla si la información puede o no ser utilizada? ¿En la empresa? ¿En Europa? Virtualmente, podría afirmarse que el perímetro se extendió hasta un lejano país, a pesar de que las políticas que el propio perímetro posee no se transportan ni con el gerente, ni con la computadora, que posteriormente volverá a ser conectada a la red de la compañía.

Ese viejo concepto, entonces, queda obsoleto. El perímetro en las redes corporativas es, por lo menos, difuso, y eso implica una serie de amenazas y riesgos que deben ser abarcados con un nuevo paradigma en la forma de comprender la seguridad de la información en las redes corporativas.

El nuevo escenario

Como se mencionaba anteriormente, la protección basada en el perímetro, al menos tal como era concebida, es un método insuficiente para proteger las redes corporativas. A continuación se detallan los principales componentes que han modificado el escenario, aquellos que han dado lugar a esta era de la conectividad.

Hardware

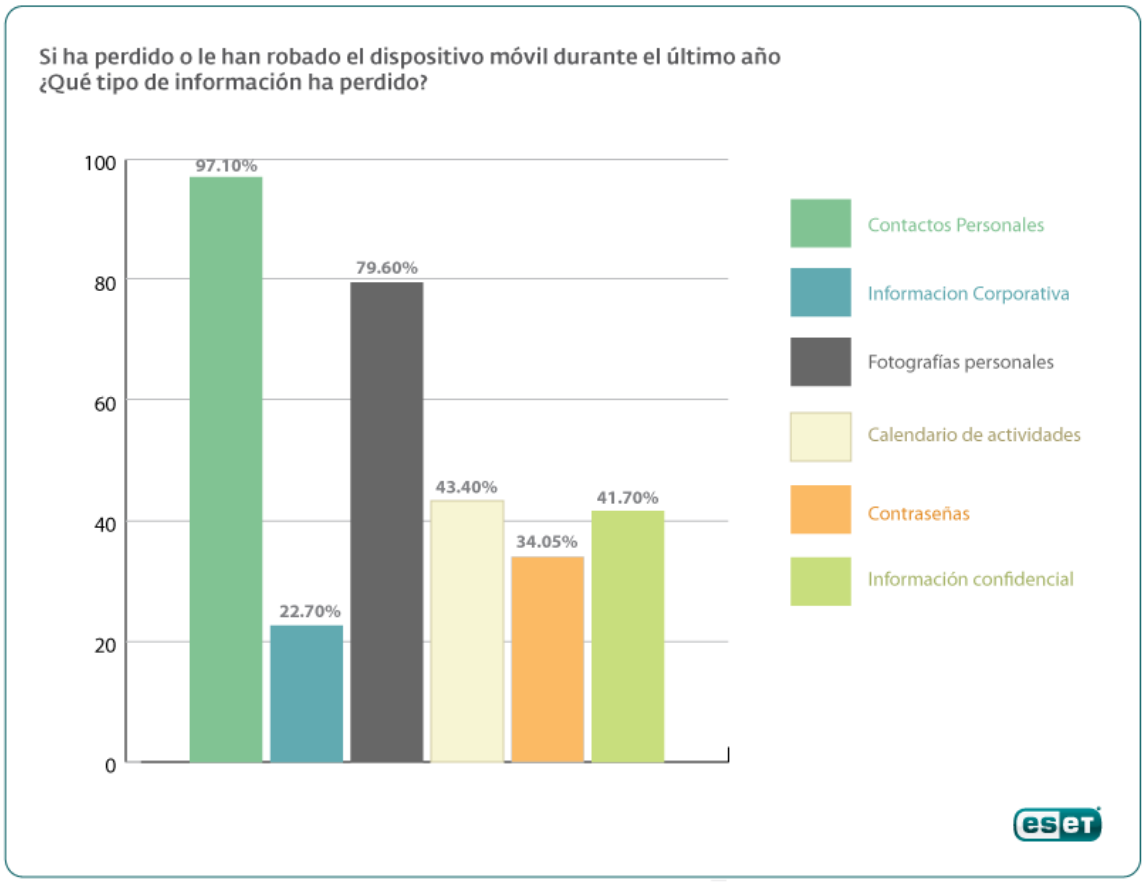
En primer lugar, nuevos dispositivos han comenzado a ser utilizados por los diversos integrantes de la organización. Estos poseen la particular característica de poder transportar información (potencialmente sensible) desde y hacia la organización a través de las personas, que se convierten en **usuarios móviles**, que utilizan información de la organización 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, en el tren, en el avión, entre otras posibilidades.

Algunos dispositivos de hardware que presentan estas características son:

- Dispositivos USB: todo tipo de memorias con conector USB, que permiten a los usuarios llevar y traer información a la red empresarial, pero que a la vez son conectadas en computadoras que no poseen las medidas de seguridad que se utilizan dentro de la red.
- *Laptops*: las computadoras portátiles permiten no sólo transportar información hacia fuera del perímetro, sino también la alteración de la misma, y la conexión 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.
- *Smartphones*: una gama de teléfonos de última generación, que poseen funcionalidades similares a las laptops, presentando las mismas características ya expuestas, sumadas a algunas particularidades específicas: facilidad para que el dispositivo sea robado o perdido y facilidad para conexión en redes inalámbricas (*wireless, bluetooth*, Internet). Según una encuesta realizada por ESET Latinoamérica, a la fecha el 47,3% de los encuestados manifestó contar con un dispositivo móvil de este tipo.

Todos estos dispositivos son susceptibles de una serie de ataques como robo físico, robo de información, alteración de la misma, infección por códigos maliciosos, robo de identidad, accesos no autorizados, y otros.

El 40% de los usuarios de Latinoamérica manifestaron haber sufrido extravío o robo de su dispositivo móvil en el último año, y han indicado en tal caso haber perdido información sensible, como se indica en el siguiente gráfico:



En estos casos, donde el dispositivo se ha perdido o ha sido robado, es importante contar con la posibilidad de que la información confidencial contenida en dicho equipo no sea accedida por terceros, como una de las funcionalidades incorporadas en ESET Mobile Security que permite borrar los datos del dispositivo extraviado, además de configurar una determinada cantidad de tarjetas SIM que se pueden utilizar en ese teléfono.

Conectividad

En los últimos años se han modificado (en realidad, extendido) las posibilidades de conectarse a Internet, por medio de los dispositivos de hardware antes mencionados.

Luego de la evolución de las conexiones por módem hasta la popularización de la banda ancha, donde se ven aumentadas las velocidades de transmisión, y la posibilidad de conectarse a redes permanentemente, aparecen los nuevos enlaces de **banda ancha móvil** (por ejemplo GPRS o 3G) que permiten la conexión continua de dispositivos móviles como computadoras portátiles o *smartphones*.

Con la banda ancha, las redes estaban 24 horas conectadas. Con la banda ancha móvil, **el usuario está 24 horas conectado**.
En Latinoamérica, la mitad de los usuarios acceden a las redes sociales desde sus dispositivos móviles y más de la mitad utilizan un sistema de mensajería instantánea (chat). Mientras que sólo 2 de cada 10 ya utilizan el home banking desde el móvil, el 80% ya accede a su correo electrónico con su teléfono.

Software

Para completar los cambios impuestos en hardware y conectividad, una serie de herramientas de software permiten dar soporte a estos, proporcionando a los usuarios herramientas que les permitan trabajar y optimizar los enlaces móviles en los diversos dispositivos.

Por ejemplo, se proveen herramientas para mantener sincronizada la información tanto en computadoras de escritorio, como *laptops* o *smartphones*. De esta forma, el usuario puede trabajar con cualquier hardware, en cualquier entorno, y con cualquier conexión, y estar utilizando la misma información. El 66.5% de los usuarios encuestados por ESET Latinoamérica manifestaron sincronizar el dispositivo móvil con otros equipos.

También han evolucionado las tecnologías de acceso remoto, como redes privadas virtuales (VPN por las siglas en inglés), que permiten conectarse a otras redes como si el usuario estuviera dentro del área de trabajo, por lo general utilizando Internet como infraestructura para tal fin. Esto permite a las empresas contar con nuevos métodos de trabajo remotos, conexiones de clientes, proveedores, partners, y cientos de usos más con metodologías diversas.

Otros riesgos asociados

¿Qué cubre el perímetro cuando existe un teletrabajador conectándose a la red corporativa desde su casa? Si en el mismo hogar hay una red inalámbrica donde se conectan los vecinos, ¿es un problema por

el que la empresa debería preocuparse? Cuando un proveedor se conecta remotamente a los sistemas de la organización, ¿los problemas de seguridad de esa otra red corporativa son un problema ajeno como lo eran anteriormente?

Además, nuevas tecnologías de *Cloud Computing* [1, 2] permiten la utilización de servicios directamente desde Internet. Sin embargo, en estos servicios suele transmitirse y volcarse información sensible para la empresa, que puede ser almacenada por un proveedor en servidores ajenos a la organización. ¿Es la seguridad de estos servidores un problema de seguridad de la empresa?

Como puede observarse, este nuevo escenario ofrece nuevos problemas y riesgos que deben ser considerados desde el punto de vista de la seguridad.

La combinación entre los componentes de hardware, de software y los nuevos servicios y herramientas de conexión a Internet, son los que definen, en conjunto, la era de la conectividad. De esta forma se hacen posibles nuevos ataques o se producen nuevas vulnerabilidades por donde puede ser comprometida la seguridad de la información de la organización.

Desafíos y problemáticas

¿Cuáles son las problemáticas que se presentan con este nuevo escenario? Como se ha mencionado anteriormente, la introducción de nuevos componentes (sean de hardware, software o conectividad) presenta nuevos desafíos. A continuación se resumen las principales dificultades para implementar seguridad (al menos con el viejo paradigma de protección) en la era de conectividad. El impacto sobre la seguridad incluye variables como:

- **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, aunque con la dificultad de que puede no contarse con la administración necesaria (computadoras personales, servidores externos, entre otros).
- **Dificultad para mantener el monitoreo sobre el hardware**: los nuevos componentes de hardware "salen y entran" de la red, conectándose de manera temporaria. ¿Cómo mantener el control sobre los mismos? Cuando estos dispositivos están fuera de la red, incluso sin conectividad, no es posible monitorear 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 empresa**: 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 estos poseen sobre sus servicios, y que incidirán directamente sobre la información sensible de la empresa.

Nuevo escenario de defensa

Presentada la problemática, **¿cómo definir un esquema de seguridad en la era de la conectividad?** La respuesta es muy sencilla: es necesario cambiar el paradigma con el que se define la seguridad de la información en la empresa. Ante un escenario más complejo, que presenta las dificultades antes expuestas, el esquema de seguridad perimetral es insuficiente, y debe exponerse un nuevo modelo, que debe estar basado en la re-definición de los tres ejes involucrados: tecnologías, gestión y educación.

Tecnologías de seguridad

Nuevas tecnologías comienzan a dar respuestas a este nuevo escenario, y las empresas no deben ser reticentes a implementarlas. Por ejemplo, a pesar que ya existen **soluciones de seguridad para dispositivos móviles como ESET Mobile Security** [3], gran parte de las empresas siguen considerando sólo la protección de computadoras de escritorio [4]: mientras que el 96% de los usuarios manifestaron estar preocupados por la seguridad en dispositivos móviles, el 74% declaró que no utiliza ninguna solución antivirus.

Por otro lado también existe la tecnología capaz de verificar cada vez que un usuario o dispositivo sale, ingresa o vuelve a la red corporativa de modo tal de controlar que la información sensible de la compañía no sea dañada, accedida o alterada sin autorización; así como también productos que permitan eliminar la información sensible de un dispositivo móvil si este es extraviado o robado. como es el caso de ESET Mobile Security[4].

Es necesaria la adopción de estas nuevas tecnologías para dar protección eficiente en estos tiempos de cambios. Los dispositivos desconectados de la red corporativa, pero con información sensible, deben ser protegidos.

Gestión de la seguridad

La gestión de la seguridad debe ser considerada con mayor importancia de 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.

Por ejemplo, los Contratos de Confidencialidad o de Calidad de Servicio dan una respuesta de gestión al control de la seguridad en servidores externos o de proveedores de servicios.

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. Al diversificarse el escenario, deben seleccionarse correctamente las tecnologías, para minimizar los costos e incluso calcular el retorno de inversión oculto que estos pueden representar para la organización. Esto sólo es necesario si se definen las herramientas de gestión para tal fin.

En resumen, las herramientas de gestión dan soporte a las tecnologías de seguridad que sean utilizadas.

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 concientización.

Educar a los usuarios permite involucrar a estos en el proceso de proteger los activos de la empresa. Al poner este nuevo modelo el foco en el usuario, éste debe ser conciente de la importancia de su rol en la seguridad de la información de la organización. Para ello la empresa debe establecer capacitaciones y concientización en forma periódica y regular, adaptadas a las características de la organización y el rol de los empleados y de acuerdo con la preocupación demostrada en educar al usuario [5].

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**.

Conclusión

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.

Sin embargo, aún en este entorno debe protegerse la información de la empresa, y es necesario un cambio de paradigma en la forma en que se abarca la seguridad de la información en la red corporativa.

A tal fin es imperioso comprender que la seguridad no puede ni debe ser la sumatoria de implementaciones aisladas de tecnologías, sino que hoy, más que nunca, debe transformarse en la combinación cuidada y coordinada de tecnologías (no obsoletas, modernas), herramientas de gestión (impulsadas desde los cargos más jerárquicos de la organización) y concientización (el mejor usuario es el usuario educado).

De esta forma será posible dar respuestas eficientes ante los desafíos que impone a la seguridad, la era de la conectividad.

Referencias

[1] **¿Nube o humo?**

http://blogs.eset-la.com/laboratorio/2009/09/29/computacion-nube-o-niebla/

[2] **Seguridad en *Cloud Computing***

http://blogs.eset-la.com/laboratorio/2010/02/23/seguridad-cloud-computing/

[3] **ESET Mobile Security**

http://www.eset-la.com/mobile-security/

[4] **Encuesta sobre el uso de antivirus en móviles**

http://blogs.eset-la.com/laboratorio/2009/12/04/encuesta-uso-antivirus-moviles/

[5] **ESET Security Report - Latinoamérica**

http://www.eset-la.com/centro-amenazas/2297-reporte-anual-latinoamerica