

***M
a
g
a
z
i
n
e

N
E
W
S

S
E
R
C
A
M
A
N***

sercaman 1



Nº 3 DICIEMBRE-ENERO

Tres propuestas de Charmex Internacional para digitalizar las aulas



Las **pizarras interactivas** han impulsado el crecimiento y la renovación metodológica en las aulas a lo largo de los últimos 10 años. Además de fomentar la flexibilidad, la espontaneidad y la integración de los alumnos en la clase, la PDI representa una extensión natural de las herramientas que ya se utilizan en el ámbito empresarial, como los **sistemas de participación interactivos**, y **proyectores que actúan como PDIs**.

En este escenario, la compañía **Charmex Internacional** propone al mercado educativo la oferta más vanguardista en tecnologías orientadas al aula digital. Tomando como referencia la voluntad de la firma por plantear respuestas a las necesidades más demandadas por profesores y alumnos, la compañía presenta tres soluciones: la resistente pizarra digital interactiva **StarBoard**, el innovador proyector LCD **Ultimate iPJ-AW250NM**, ambos de **HITACHI**, y el sistema de participación **TurningPoint de Turning Technologies**.

"La implementación de cualquiera de estos tres elementos de Charmex en el aula escenifica el paso siguiente en la evolución de las soluciones interactivas y las tecnológicas orientadas al mundo de la educación", señala **Gerard Usón, responsable del departamento de soluciones interactivas de Charmex Internacional.** De acuerdo con el responsable de Charmex, el avance evolutivo en tecnologías orientadas al aula digital viene encabezado por la pizarra digital interactiva HITACHI StarBoard; un dispositivo dotado de sensores ópticos que puede usarse simplemente con las manos, cuya superficie a prueba de golpes lo convierte en el más resistente del mercado, y se caracteriza además por permitir trabajar hasta a tres usuarios simultáneamente gracias a su tecnología multi-entrada.

Asimismo, el software que incluye la PDI StarBoard resulta muy intuitivo y fácil de utilizar lo cual, para los profesores, supone una ventaja ya que ponerlo en marcha y utilizarlo resulta un procedimiento muy rápido y sencillo. *"La pizarra funciona como una tableta gigante, de manera que cualquier fichero de Word, PowerPoint, Excel, o cualquier otra aplicación interactiva que haya sido elaborada en código abierto puede ser utilizada por la StarBoard",* puntualiza Usón.

La formación en el uso de las PDIs por parte del profesorado sigue siendo una de las asignaturas pendientes del sector. De acuerdo con Usón, un buen número de educadores que utilizan PDIs suele realizar una explotación baja de las posibilidades de las pizarras interactivas por inseguridad o porque nadie les ha explicado cómo utilizarlas. Para solucionar esta problemática, Charmex ha puesto en marcha un ambicioso plan de formación gratuito que se imparte online, y con tutor personal, para que cada profesor lo adapte a sus necesidades, profundice en aquellos aspectos que más le interesen, y para evitar que las pizarras interactivas que se instalan sean infrutilizadas.

Un proyector que cumple las funciones de una PDI

Para aquellos usuarios que prefieran instalar un sistema de proyección interactivo que funcione sobre cualquier superficie plana en lugar de alojar una PDI, el proyector HITACHI iPJ-AW250NM integra un conjunto de tecnologías probadas, ya existentes, para crear una solución nueva, sencilla e innovadora que ofrece gran parte de las ventajas de las "whiteboards" sin la necesidad de implementar equipos dedicados. Siempre que se disponga de una simple pared desnuda será muy fácil hacer funcionar el proyector interactivo de manera rápida y precisa a través de un sensor integrado que utiliza ondas infrarrojas y ultrasónicas, el cual transfiere la información para ser controlada por el software HITACHI Starboard, que puede incluirse en el propio paquete interactivo del cliente o sustituirlo.

A diferencia de la posibilidad de poder utilizar las manos para controlar la función de pizarra digital que permite realizar la StarBoard, el iPJ-AW250NM utiliza únicamente un lápiz interactivo que transfiere la información de la actividad que se produce sobre la pizarra, al tiempo que accede al manejo de herramientas, archivos interactivos flash y los elementos más habituales del aula. La función mejorada del software Ajuste Perfecto del sistema brinda ahora la posibilidad de ajustar del proyector en ocho puntos, garantizando unas imágenes e interactividad perfectas. Asimismo, el software de gestión que incorpora la serie Ultimate permite el control de múltiples proyectores a través de la red facilitando, de este modo, la monitorización y la dirección de instalaciones dotadas con varios equipos.

El diseño inteligente del iPJ-AW250NM consigue optimizar el flujo de aire frío a su alrededor; un aspecto que, en combinación con otros factores como el hecho de estar construido con piezas de larga vida útil, la incorporación de un filtro híbrido, y una lámpara cuya vida supera las 5000 horas, convierten al nuevo dispositivo de proyección interactiva de Hitachi en la solución más versátil, económica, y amigable con el medio ambiente del mercado.

Complementando la oferta más avanzada y versátil para el aula digital, Charmex propone la solución TurningPoint de Turning Technologies; el sistema interactivo de respuestas que es capaz de crear un ambiente único de aprendizaje, elimina la corrección manual de las tareas, y contribuye considerablemente a la mejora del rendimiento del alumnado. TurningPoint es una solución completamente interactiva, la más avanzada de su clase y más fácil de usar que reúne las respuestas y convierte de inmediato los resultados en puntuaciones de pruebas, cuadros y gráficos. La versatilidad de TurningPoint proporciona un apoyo decisivo al ámbito educativo al ser capaz de incrementar notablemente del nivel de interactividad entre el profesional docente y sus alumnos.

En este sentido, Gerard Uson, señala que *"el sistema de respuesta interactiva marca una diferencia real ya que, con dicha tecnología, las asignaturas de matemáticas, lectura y ciencias, incrementan sus respectivos porcentajes de aciertos en torno a un 50%."* Asimismo, TurningPoint es aplicable a todo tipo de materias de estudio y de niveles de enseñanza tanto en escuelas como universidades e institutos. Con todo ello, TurningPoint es el único sistema de votación interactivo que se integra al cien por cien con las aplicaciones Windows de Microsoft, dándole la capacidad de crear, expresar y evaluar sin tener que salir del programa de presentaciones.



Invertir en Seguridad informática no es una opción

Por Israel Zapata Palacio, Director Técnico Secura IT.

Hoy en día debemos ser conscientes de que la seguridad informática es un área empresarial en la que es necesario invertir, puesto que las consecuencias de no hacerlo pueden ser devastadoras.

Hemos dejado atrás la era de la información y estamos en la era de la conexión. Almacenamos toda nuestra información en Internet y por eso el acceso a esos datos ha de estar protegido y garantizado. Así las cosas la pregunta que surge es: ¿Qué causa pérdidas a las empresas? Las respuestas, a continuación.

1. La navegación no controlada de los empleados. El acceso a Facebook, chats, periódicos reduce considerablemente el tiempo efectivo de trabajo del personal. Un estudio realizado por Secura ha arrojado que, de media, cada persona pierde 48 minutos al día en navegación personal (una empresa de 100 empleados con un sueldo medio de 25.000€ puede concluirse que al año pierde 230.769€ por este motivo).

2. Fuga de información. Más del 70% de los robos y fugas de información provienen de los propios empleados. Hay dos métodos para sacar información fuera de la empresa: una es Internet, ya que cualquiera puede enviarse un correo con información confidencial a una cuenta privada o incluso subir un adjunto a su correo web personal. La otra son dispositivos de almacenamiento por USB. Ambos métodos se consiguen controlar con los sistemas DLP (data loss prevention) que identifican la información confidencial, evitan su envío por Internet y prohíben el uso de memorias o módems USB ajenos a la compañía.

3. Ataques hackers. Las historias de Sony o Nintendo son las más sonadas pero no las únicas. Se afirma que las pérdidas por robos informáticos ya superan a las sufridas por robos físicos. Tendemos a pensar que no somos objetivo de un ataque, pero toda empresa está en el punto de mira. De hecho, las mafias organizadas usan a hackers para robar fácilmente pequeñas cantidades a miles de Pymes, en lugar de robar miles de millones a las grandes multinacionales que invierten mucho en seguridad y están protegidos.

La mayoría de los firewalls actuales tienen ya incluidos detectores de intrusos y son asequibles para todo tipo de empresas. Son los llamados firewalls UTM (Unified Threat Management) que reúnen muchas funcionalidades en un solo equipo.

Poco a poco se empieza a tener conciencia en el ámbito empresarial de que hay que usar los sistemas de información con garantías de disponibilidad, confidencialidad e integridad. La inversión en seguridad debería hacerse de manera progresiva aunque obligada para reducir así los riesgos tecnológicos a los que estamos expuestos y potenciar al máximo nuestra productividad.

Conoce cómo proteger tu móvil Android de la amenaza de los virus

La fuerte expansión de los smartphones con sistema operativo Android ha dado pie a un impresionante desarrollo de **malware** orientado para esta plataforma. Esto ha despertado la reacción de varias empresas de seguridad informática en forma de versiones móviles de sus conocidos **antivirus**.

Los virus se adaptan a los nuevos tiempos y ya han dado el salto a los **teléfonos móviles y tabletas**, dispositivos que han pasado a ser objetivo de los desarrolladores de todo tipo de malware. Encontrarse con **virus, spyware o troyanos** es, por desgracia, cada vez más habitual en las plataformas móviles. Pero si hay un segmento de usuarios más afectados por la proliferación de software malicioso es el conformado por la comunidad Android.

En los últimos meses hemos asistido al apogeo de nuevas amenazas para los terminales con el sistema operativo de **Google**. Los datos impresionan: desde el pasado mes de julio [las amenazas han crecido un 472%](#), lo que significa que en **Android Market**, la tienda de aplicaciones de la compañía, hay cinco veces más malware que hace apenas cuatro meses. Los meses de octubre y noviembre registraron datos muy significativos, con un aumento del 110% y 111% respectivamente.

El desarrollo de estos virus, que pueden tanto alterar el funcionamiento del terminal como rastrear su actividad en Internet o **recopilar todo tipo de datos personales**, se ha producido gracias a la falta de protección de los usuarios así como a las numerosas imprudencias de éstos. No obstante, con el paso del tiempo hemos asistido al nacimiento de varias ofertas en forma de antivirus móviles, cada vez más necesarios ante los riesgos existentes.

Avast se une a las alternativas en el Android Market

El más conocido hasta el momento es **Lookout Security Antivirus**. Su descarga es gratuita y hasta el momento es la alternativa más utilizada por los usuarios. Asimismo, existen otras de pago como **Antivirus Pro**, desarrollada por AVG y que tiene un precio en estos momentos de 3,63 euros.

A éstas se les ha unido recientemente la versión móvil de **Avast**, el conocido antivirus **gratuito** que ha triunfado en los PC de un tiempo a esta parte. Las funcionalidades de esta aplicación son múltiples con el objetivo de maximizar la seguridad y privacidad del usuario. Se encarga de **controlar las aplicaciones** que se instalan en el terminal y detectar todo tipo de malware. Igualmente, realiza una vigilancia de las páginas por las que el usuario navega con el fin de evitar riesgos, incluye un **firewall** que detecta qué aplicaciones acceden a la Red y permite bloquear llamadas o SMS. Una de las funciones más interesantes es la posibilidad de detectar el terminal en caso de **robo o pérdida** a través de un sistema de geolocalización e incluso borrar la información almacenada en el terminal de forma remota.



Las amenazas informáticas que enfrentaremos el 2012

Fecha de publicación: 12/12/2011

**Cristián
Desde**

Buenos

Aires,

**Vera-Cruz
Argentina**

Finaliza el 2011 y es habitual empezar a proyectar cuáles serán las tendencias que veremos el próximo año en materia tecnológica. Y uno de los sectores que se vislumbran más “movidos” es el de la seguridad informática.

Así como cada día nacen nuevos dispositivos que nos sorprenden por sus características y funcionalidades, todos los días los creadores de códigos maliciosos lanzan nuevos tipos de ataques y amenazas que buscan aprovechar brechas en programas y equipos, y como siempre, las a veces permisivas conductas de los usuarios.

En este sentido, tuvimos la oportunidad de asistir a una interesante conferencia sobre esta materia organizada por la compañía ESET en Buenos Aires, donde pudimos conocer cuáles serán las tendencias en seguridad informática para el 2012.

De acuerdo al informe "Tendencias 2012: el malware a los móviles", elaborado por el Laboratorio de Investigación de ESET Latinoamérica, y dado a conocer en el evento, el próximo año los equipos móviles constituirán uno de los principales objetivos de los ciberatacantes, quienes continuarán desarrollando un gran número de ataques informáticos dirigidos especialmente a dispositivos con sistemas operativos Android. Asimismo, la evolución de las tecnologías de seguridad en los sistemas operativos de escritorio dará lugar a nuevas amenazas más complejas.

En ese sentido, de 41 nuevas variantes de códigos maliciosos para sistemas operativos Android analizadas por el Laboratorio de Investigación de ESET Latinoamérica, el 70% apareció durante el último semestre del 2011, constituyéndose como el período de mayor desarrollo de amenazas para esta plataforma en los últimos dos años. El crecimiento en la tasa de uso de dicha plataforma se presenta como uno de los principales motivos para que los cibercriminales dirijan sus esfuerzos en este sentido. Cabe señalar que según los datos arrojados por la consultora Gartner, a mediados del 2011, Android era el líder de plataformas móviles con más de 400 millones de dispositivos móviles en todo el mundo, creciendo a razón de 550 mil dispositivos por día.

Además, el aumento del impacto causado por el malware en equipos móviles se perfila también como una tendencia para el 2012 que tiene como caso testigo a DroidDream, amenaza que logró más de 250.000 descargas desde el Android Market. El caso obtuvo tanta repercusión que Google decidió desinstalar remotamente la aplicación de todos los sistemas infectados por dicho código malicioso. A su vez, todos los usuarios cuyo dispositivo móvil había sido comprometido fueron notificados a través de un correo electrónico.

"A pesar de las diferencias entre el mundo del móvil y el de los equipos de escritorio en cuanto a cantidad de dispositivos y de amenazas, hoy en día los creadores de aplicaciones maliciosas están encontrando en Android muchas de las características que años atrás encontraron en Windows XP. El crecimiento en el market share y la posibilidad de propagar códigos maliciosos en repositorios, oficiales o no, entre otras características, posicionarán a Android como el uno de los objetivos privilegiados de los desarrolladores de códigos maliciosos durante el 2012", destacó Sebastián Bortnik, Coordinador de Awareness & Research de ESET Latinoamérica.

Por otra parte, la evolución de las tecnologías de seguridad en las plataformas de equipos de escritorio y el progresivo reemplazo de Windows XP por Windows 7 exigirá a los ciberatacantes el desarrollo de amenazas más complejas desde el punto de vista tecnológico. En la era de Windows XP, muchas amenazas únicamente sobrescribían una entrada de registro o escribían un archivo para hacer daño en el sistema, mientras que en la actualidad los nuevos códigos maliciosos deberán incorporar también funcionalidades destinadas a lograr la ejecución en el sistema, antes del daño propiamente dicho.

Por este motivo, para el 2012 aparecerán también más códigos maliciosos con capacidades de vulnerar los sistemas de firmado digital con los que cuentan los sistemas operativos más modernos.

“Más allá del crecimiento que se espera de amenazas más complejas desde el punto de vista tecnológico, también se ha verificado un gran desarrollo en la tendencia opuesta: códigos maliciosos extremadamente sencillos que apelan simplemente a la Ingeniería Social han proliferado durante el 2011 y continuarán propagándose durante el próximo año. Se trata, por ejemplo, de troyanos bancarios de la familia Qhost que al ejecutarse en el sistema, modifican un archivo de texto para que el atacante robe las credenciales bancarias de los usuarios”, agregó Bortnik.

En línea con esto, el panorama de amenazas presentado para el 2012 incluirá con menor frecuencia amenazas de alta complejidad y gran impacto junto con ataques sencillos y de fácil acceso para los desarrolladores, con un grado mayor de masividad. Por otra parte, pueden esperarse ataques generados localmente en Latinoamérica, especialmente de tipo hacktivista, es decir, ataques con fines ideológicos en lugar de económicos. A su vez, cabe esperar ataques a través de redes sociales y una alta tasa de propagación de troyanos bancarios, el tipo de códigos maliciosos más característico en nuestra región.

Si antes el objetivo era sólo el computador, la aparición de nuevos aparatos como netbooks, tablets y smartphones, ha modificado el target de los desarrolladores de código malicioso. A juicio de Bortnik “de una u otra forma todas las amenazas en materia de cibercrimen están relacionadas con las evoluciones tecnológicas del último tiempo”.

Y frente a este escenario, uno se pregunta si para el próximo año se espera que el usuario latinoamericano adquiera mayor conciencia para evitar ser afectado por ataques informáticos. La respuesta de Sebastián Bortnik es que "para las personas existen varias instancias de orientación y prevención, y la tecnología también ayuda en esa tarea, pero es vital que los usuarios sean conscientes de la necesidad de implementar las herramientas, saber configurarlas y actualizarlas. Yo no tengo duda de que los usuarios van a estar más atentos y conscientes el próximo año, pero esa conciencia debe ir más rápido de lo que evolucionan las amenazas. También es importante destacar que falta más información y llegar a más usuarios con los mensajes de prevención. Por mi experiencia diaria, no me cabe duda que la educación funciona, pero el desafío es ampliar el alcance de la educación en seguridad informática. Por ello, es fundamental el trabajo coordinado entre los investigadores, los medios, los docentes y los gobiernos".

El mercado mundial de impresión crece un 1,6% en el tercer trimestre

Según datos de la [consultora ID](#), el mercado mundial de impresión ha crecido un 1,6% en el tercer trimestre de 2011, con **31,3 millones de unidades vendidas**. Las impresoras suponen el **66% de las ventas** entre los meses de julio a septiembre. Dentro de ellas, las que usan tecnología láser color, se llevan la palma con un crecimiento en ventas del **24,1%** en relación con el tercer trimestre de 2010.



IDC ha destacado que los dispositivos de chorro de tinta, fundamentalmente los multifuncionales, son los que más se venden, ya que alcanzan los **19,6 millones de unidades** en todo el mundo. En el tercer trimestre siguen en segunda posición las máquinas monocromas láser, que suponen un **29% del mercado**.

Respecto a los fabricantes que las suministran, el líder seguiría siendo HP con **13,46 millones** de equipos vendidos en el trimestre, un **0,8% más** que el mismo periodo del año anterior. Le seguiría Canon, con 5,67 millones (5,2% más) y Epson, con **3,94 millones** (caída del 9,4%). En cuarto lugar se encuentra Samsung, con **1,8 millones comercializados** (un incremento del 8,3%) y, en quinto puesto, Brother, con 1,73 millones y un aumento del 7,5%.