

Modelo transversal de seguridad

Eva Rodríguez, consultora senior de SATEC (www.satec.es) nos señala la necesidad de reforzar y consolidar los planes de protección de las infraestructuras críticas de las organizaciones, ante el aumento de la dependencia de las Tecnologías de la Información.

Según Eva Rodríguez, "A día de hoy la gestión de la seguridad está fundamentalmente enfocada hacia una seguridad informática, normalmente con políticas disjuntas entre los diferentes departamentos implicados – gestión en silos de información – esto hace que se incrementen gastos, redundando funciones y trabajo, es decir no hay una visión transversal de la misma, lo que hace que se trabaje de una forma ineficiente tanto en recursos económicos como en procesos."

Asimismo, destaca la importancia de la nueva ley de Protección de Infraestructuras Críticas (PIC) al aglutinar los diversos procesos y procedimientos que conforman una política de seguridad,

permitiendo mantener como país todos los servicios públicos de interés general sustentados por las infraestructuras público o privadas.

En este contexto apunta a la necesidad de cambiar la cultura de seguridad para optimizar los recursos y ahorrar y también para ser más eficientes, logrando un nivel óptimo de seguridad y gestión.

Como los principales factores que inciden en la vulnerabilidad de las empresas, la consultora de SATEC destaca la limitación de los recursos dedicados y el recorte del presupuesto dedicado a la prevención y seguridad, que se ha agudizado por el drástico aumento de su dependencia de las TIC; y la ausencia de una política global de seguridad que abarque transversalmente todas las infraestructuras de las organizaciones.

Entre sus recomendaciones para garantizar la adecuada protección de las Infraestructuras Críticas, Eva Rodríguez destaca la importancia de definir una política de seguridad integral de la organización. Para

ello, es necesario analizar los riesgos de la infraestructura para identificar las medidas a implantar y garantizar la continuidad de los servicios esenciales, así como revisar los planes periódicamente para que se puedan mantener actualizados.

En palabras de la consultora de SATEC, "Es necesario cambiar la cultura de seguridad de las organizaciones, para optimizar los recursos, ahorrar costes y mejorar la eficiencia".

"Normalmente, las organizaciones tienden a centrar la seguridad de las TICs de manera aislada, como por ejemplo, en la informática. Sin embargo, el escenario de las redes de seguridad ha cambiado y es necesario proteger toda la red de activos y sistemas de datos críticos. En la actualidad, las iniciativas pierden fuerza por no estar centralizadas a través de un Responsable de Seguridad y Enlace que permita aunar esfuerzos y comunicar las acciones dentro de la organización", ha añadido.

EmO Center

Microsoft, con la colaboración de Intel, ha dado un nuevo paso en su apuesta por experimentar con la tecnología más vanguardista del mercado gracias a la remodelación que ha llevado a cabo en su conocido EmO Center, es decir, el Centro Avanzado de Demostraciones de Tecnología Microsoft. Microsoft continuará utilizando esta sala situada en sus propias oficinas de Pozuelo de Alarcón (Madrid) para mostrar sus avances más destacados en materia de software sobre soluciones de Intel en entornos de movilidad, gestión remota y seguridad así como los desarrollos conceptuales y los últimos prototipos salidos de los laboratorios de investigación de Microsoft Research.

"Desde que fuera inaugurado hace seis años, concretamente el 21 de octubre de 2005, el EmO Center se ha distinguido por su intensa actividad, albergando continuas demostraciones

de casos prácticos de las soluciones más avanzadas para cada tipo de organización o sector de actividad", recuerda David Negrete, director de la unidad de negocio de Productividad y Colaboración de Microsoft Ibérica, que también se refiere a la propia evolución de la sala: "En este periodo su funcionamiento ha variado desde las demostraciones conceptuales de sus inicios, en las que trataba de anticipar de un modo totalmente interactivo cómo sería el escritorio del futuro, hasta las actuales, que se llevan a cabo sobre tecnología real que está al alcance de cualquier empresa".

El EmO center estará dotado de las más avanzadas soluciones hardware y software integradas y se realizarán sesiones prácticas demostrando cuál es la plataforma empresarial o puesto de trabajo más idóneo: "Debe ofrecer

rendimiento inteligente, colaboración avanzada, seguridad mejorada y capacidad de gestión integrada con el objetivo de reducir costes y aumentar la productividad del empleado", comenta Agustín Gallego, Director de Desarrollo de Negocio y Alianzas de Intel Corporation Iberia.

Estas sesiones son las denominadas Customer Immersion Experience (CIE), que se caracterizan por ser totalmente interactivas así como por estar impartidas por especialistas del Centro de Productividad de Manresa. "En las sesiones antiguas había que seguir un guión para llevar a cabo la demo, mientras que en éstas el guión puede ir variando según lo desee el cliente, gracias a que los productos son reales y al apoyo que estamos recibiendo por parte de Intel", añade el director de la unidad de negocio de Productividad y Colaboración de Microsoft.