Publicado en Ciudad de México el 14/11/2016

# [CompTIA apoya la cultura de ciberseguridad](http://www.notasdeprensa.es)

## Seis pasos para crear una cultura de propiedad de seguridad que pueden ayudar a marcar el tono para una fuerza de trabajo responsable y más alerta

 Seis pasos para crear una cultura de propiedad de seguridad Todd Thibodeaux, Presidente y Director General, CompTIA El estado de la ciberseguridad corporativa es todo menos estático. Con la diversificación de la lista de amenazas potenciales, los riesgos son mayores para asegurar los sistemas y datos de una compañía. Mientras que el costo promedio de violaciones de información crece (actualmente estimado en 4 millones de dólares ($4 million), el hambre de riesgos de los líderes de negocios disminuye. Sin embargo, menos de la mitad de los profesionales en seguridad de la información opina que las defensas de sus compañías están a la par, de acuerdo a estudios (research) de CompTIA. Contrario a lo que algunos líderes de negocios puedan creer, proteger la infraestructura y la propiedad intelectual de su organización no empieza al invertir en un cortafuegos (‘firewall’). Empieza incorporando la ciberseguridad a la cultura de su compañía. La tecnología toca a todos los empleados dentro de una organización, no únicamente a aquellos en el departamento de TI. La seguridad no debe ser diferente, con un compromiso que se impregne de arriba a abajo. Aquí encontrarán seis pasos que pueden ayudar a marcar el tono para una fuerza de trabajo responsable y más alerta: 1. Reconsidere la estructura de su Grupo Directivo: una cosa es crear un cargo de Director de seguridad o Director de seguridad de la información, pero a quien esa persona reporta puede influenciar la estrategia de seguridad de su organización. Permitir que su líder máximo de seguridad reporte directamente al Director General, beneficia con mayor visibilidad las operaciones de la compañía y la toma de decisiones. También envía un mensaje más claro a través de la organización de que la ciberseguridad no está aislada en el departamento de TI. 2. Dar prioridad a los conocimientos del usuario final: aunque muchos profesionales TI piensan que los empleados de sus organizaciones cuentan con un conocimiento sólido de seguridad, encuestas e incidentes de la vida real nos cuentan una historia diferente. Globalmente, más de la mitad de las organizaciones reportan que un error humano es el factor principal de las violaciones de seguridad e incidentes relacionados. El problema de raíz es la falta de conocimiento del usuario final. Las sesiones “Cibersecurity 101” durante la capacitación de bienvenida a la compañía de los empleados no son suficientes para instalar hábitos sólidos. Los líderes de negocios deben demostrar su apoyo a capacitación sólida para el usuario final – de cursos electrónicos continuos a ejercicios simulados de ataques cibernéticos – y respaldarse con los recursos financieros necesarios. 3. Establecer las métricas correctas: uno de los retos más grandes en la implementación de iniciativas nuevas es vencer la creencia de que las estrategias y recursos actuales son “suficientemente buenos.” Le tecnología de la información y los ejecutivos de seguridad pueden y deberían hacer más para asegurar que el protocolo de defensa de sus organizaciones tiene sus raíces en hechos y no en sentimientos. Asociándose con consejeros expertos, pueden desarrollar caminos para medir la eficacia de sus esfuerzos de seguridad actuales, y compararlos con estándares de la industria. 4. Reunir procesos de negocios y tecnología: elevar la ciberseguridad a un asunto agnóstico departamental va más allá de la implementación de prevención de pérdida de información o de identificar soluciones administrativas de acceso. Involucra formalizar procesos nuevos (y actualizar los existentes) a través de una combinación de lentes de negocios y de TI. La administración de riesgos y cumplimiento, selección de proveedores nuevos y la capacitación en seguridad del usuario final no pueden ser prácticas que los departamentos TI crean e imponen a sus colegas. La línea de líderes de negocios debe estar igualmente involucrada en la creación de estas políticas para asegurar que se ejecutan efectivamente. 5. Promover una nueva perspectiva sobre el gasto para seguridad: la seguridad es una rebanada del presupuesto de TI, una que los líderes de negocios históricamente ven como algo que debe contenerse, invirtiendo en ella únicamente cuando sea necesario en tiempos de una crisis real o inminente. Las organizaciones que se esfuerzan en promover una cultura de seguridad necesitan más posturas proactivas hacia su estrategia y presupuesto. Esto significa colocar a la ciberseguridad como una oportunidad de inversión y no como un artículo de línea reticente. 6. Incentivar responsabilidad: luchar por apoyo a nuevas políticas y promover el conocimiento de la ciberseguridad puede fácilmente encontrar resistencia y poco interés, por lo que las organizaciones deben ser creativas. Ofrecer beneficios a los departamentos o equipos que participan colectivamente en la mayoría de oportunidades de educación en seguridad, puede motivar al personal no técnico a tomar en serio la seguridad. De igual manera, los empleados que ofrecen nuevas ideas de seguridad o llaman la atención sobre posibles fallas de seguridad, deberían recibir reconocimiento público en la compañía para motivar iniciativas similares dentro de la organización. Las organizaciones están tan seguras como su contraseña más débil, procesos de administración o hábitos del usuario final. Cuando los ejecutivos traten a la ciberseguridad como un principio corporativo más que como un deber de TI, todos los empleados tendrán una razón de apoyo a la causa.

**Datos de contacto:**

Rocío Sandoval Garrido

CompTIA México

55 56882685

Nota de prensa publicada en: [https://www.mexicopress.com.mx/comptia-apoya-la-cultura-de-ciberseguridad\_1](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Ciberseguridad Recursos humanos



[**http://www.mexicopress.com.mx**](http://www.notasdeprensa.es)