4 hábitos que tu empresa debe adoptar para no comprometer la seguridad de los clientes

- *El 53 % de las empresas busca integrar a sus equipos de seguridad y desarrollo; los sistemas CMS (Content Management System) pueden ser clave para alinear una estrategia comercial, tecnológica y de seguridad.*

La seguridad se está posicionando, junto a las ventas *online* y la innovación, como **una de las mayores prioridades de la transformación tecnológica** empresarial: los recientes anuncios de Google respecto a la eliminación de *cookies* de terceros en Chrome, su navegador, son una de las grandes medidas que se están tomando para hacer del espacio digital un lugar más seguro. No obstante, esto también **está cambiando la manera cómo las empresas conectan con los consumidores**.

> "Frente a este escenario, las compañías ahora están por enfrentar un reto mayor: diseñar nuevos tipos de experiencias 360º para entender a los consumidores, aunque ahora tendrán que hacerlo sin comprometer la privacidad de la información, tanto interna como externa; **la seguridad empezará a formar parte de la estrategia comercial** y tecnológica", explica Shelley Pursell, **Directora de Marketing en Latinoamérica e Iberia para HubSpot**, plataforma CRM que ayuda a las empresas a alinearse con el éxito de sus clientes.

De acuerdo con una encuesta de VMWare, el 53 % de las empresas **ya visualiza una alineación de los equipos de seguridad, desarrollo y ventas** en un lapso de tres años. Para Pursell, los siguientes hábitos no solo permiten a las empresas ofrecer mayores seguridad, sino que también son una buena forma de empezar a alinear las funciones de cada uno de estos departamentos a fin de crear mejores experiencias para sus clientes:

1. **Administra el acceso a la información**

Es importante comprobar que tu empresa clasifique de manera adecuada los datos que estás administrando, principalmente los relacionados a tus clientes. Los sistemas de gestión de contenidos (CMS) hoy **se antojan como una alternativa para la alineación de la estrategia de seguridad y comercial** gracias a sus funciones de seguridad como SSL, cortafuegos de aplicaciones web y una red de distribución de contenidos (CDN) alojada en todo el mundo, lo que permite a los encargados de seguridad del sitio configurar controles de acceso a datos fácilmente, mientras marketing se centra en crear mejores experiencias para los usuarios.

2. **Identifica tus activos de TI**

Lo primordial es identificar los dispositivos que conforman la red de tu compañía (impresoras, estaciones de trabajo, teléfonos inteligentes, routers, etc.), así como cualquier sistema de terceros. Una vez lo consigas, **considera reducir la complejidad de equipos**, y asegurarte de que la mayoría tengan sistemas operativos compatibles, pues esto facilita el seguimiento de parches y actualizaciones de seguridad.

3. **Contempla riesgos**

Una de las maneras más efectivas de hacerlo es mediante una lista que contemple identificación de amenazas previas, determinación del riesgo y su impacto, clasificación de probabilidad y el cálculo de la calificación de riesgo. También puedes priorizarlos en función de la gravedad y la facilidad de reparación con el fin de cerrar las brechas más grandes en tu plan de ciberseguridad.

4. **Establece un plan de respuesta**

Una parte importante de la estrategia de seguridad es el plan de respuesta a una filtración, el cual debe ajustarse en función de la naturaleza del incidente y los recursos que tiene disponibles. No obstante, contar con un sistema de detección de intrusiones (IDS) es una buena práctica para contener, erradicar, recuperar la información e identificar nuevos eventos en la seguridad de datos.

Actualmente, las personas están tomando mayor conciencia acerca de cómo se utiliza su información en el espacio digital. Medidas como la eliminación de *cookies* de terceros en Chrome, **están cambiando las reglas del juego** y, ante ello, es importante que las empresas empiecen a repensar su crecimiento, poniendo la seguridad del usuario al centro de todo.