El Comercio Electrónico en tiempos de Coronavirus:
5 áreas de riesgo que las compañías no deben descuidar.

En los últimos años, el incremento del uso de la tecnología en todos los ámbitos de la sociedad ha aportado al crecimiento del comercio electrónico en Ecuador y el mundo. Según la Cámara Ecuatoriana de Comercio Electrónico, en enero de 2020 nuestro país presentaba números superiores al promedio global en aspectos como: uso de Internet, uso de dispositivos móviles y uso de redes sociales.

Por: Fernando Fernández
Gerente de Risk Assurance de PwC Ecuador

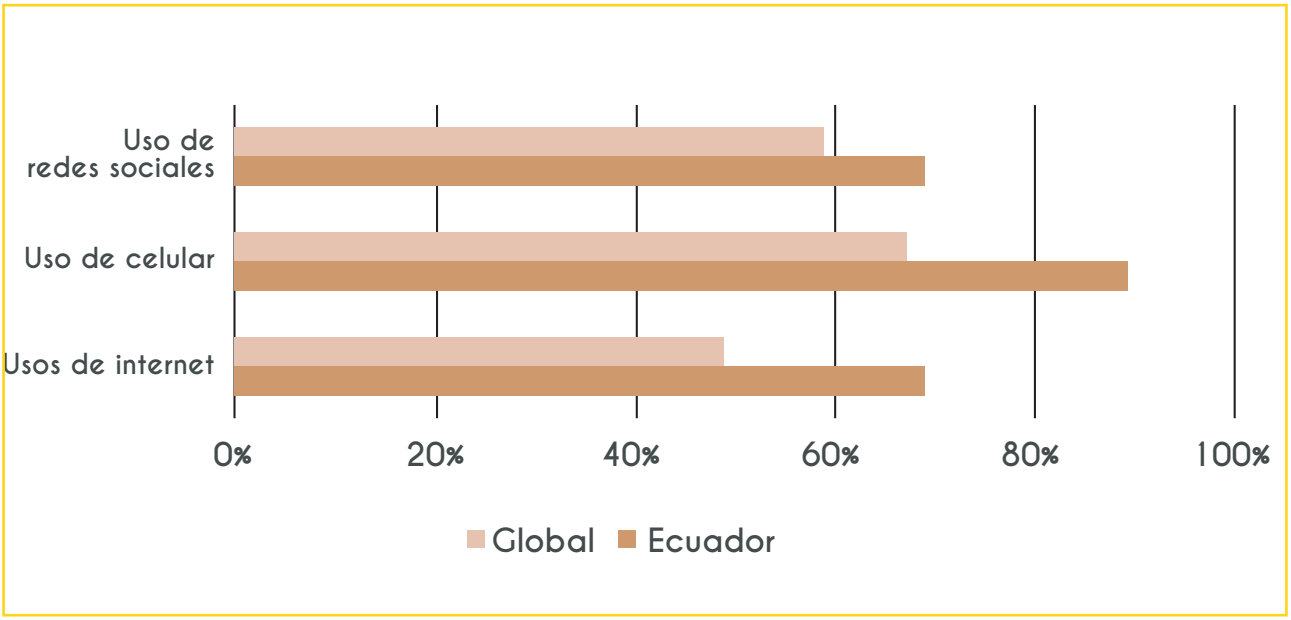
El panorama de por sí se mostraba favorable y pintaba bien en el mediano plazo, llegando a estimarse que para el año 2023, el e-commerce representaría al menos el 21% de las ventas a nivel global según datos de Stackline.

Sin embargo, Covid-19 llegó para cambiar muchas cosas. Por un lado, ha ocasionado importantes pérdidas y gran incertidumbre en muchos sectores de la sociedad; no obstante, en contrapartida, las medidas de aislamiento social y restricción de movilidad definidas para combatir la pandemia han sido el acelerador hacia la digitalización en muchas organizaciones.

Compañías de todo tipo y tamaño tuvieron que replantear sus estrategias de go-to-market, modificando algunos de sus procesos de negocio sobre la marcha, de manera rápida e improvisada en algunos casos, volcándose hacia los canales digitales para lograr mantener su operatividad y tratando de minimizar el inminente impacto económico.

Esta casuística ha generado que algunas áreas de riesgo sean subestimadas o desatendidas, pudiendo ocasionar un impacto mayor al de la pandemia si no se toman los recaudos o acciones correctivas.

Perspectiva digital: Global vs Ecuador



Más vale tarde que nunca: las 5 áreas que no deben ser descuidadas por las compañías que han incursionado en el comercio electrónico.

De acuerdo con la metodología de respuesta a los riesgos derivados del Covid-19 de PwC, existen al menos 5 factores claves que deben ser considerados por la Alta Dirección y funciones de Seguridad para mantener un balance apropiado entre la continuidad de las operaciones y la seguridad de la organización:

1

Controles internos:

Es posible que algunos controles sobre los procesos de negocio y de TI se hayan relajado, agilizando aprobaciones y priorizando el paso a producción de nuevos programas. Por ejemplo, se pudieron haber otorgado accesos privilegiados sin considerar una debida segregación de funciones o acceso a información sensible.

Es importante realizar revisiones de tipo detectivo para identificar eventuales saltos de controles que podrían representar un riesgo mayor.

2

Mecanismos de seguridad informática y monitoreo:

Es necesario reforzar los mecanismos de protección y monitoreo contra amenazas externas, principalmente si se han habilitado canales electrónicos accesibles desde Internet, incluyendo acceso remoto a empleados y proveedores como VPNs y plataformas colaborativas.
Verificar que se cuenta con las últimas actualizaciones del fabricante y estar alertas a amenazas de ingeniería social o phishing deben ser la prioridad.

Además, trabajar en la concienciación de los usuarios en temas de seguridad y plantear la posibilidad de realizar un hackeo ético de las aplicaciones e infraestructura no es una mala inversión en estos tiempos.

3

Métodos de pago:

Es clave identificar todos los métodos de pagos digitales que se hayan implementado. Se debe evaluar la adopción del estándar PCI-DSS en los casos que sea requerido por los medios de pago y tomarlo como buena práctica cuando no sea obligatorio.

4

Cumplimiento normativo:

Realizar un repaso por la Ley de Comercio Electrónico, Firmas y Mensajes de Datos para verificar que los nuevos canales de venta digitales están alineados con la normativa, se vuelve una revisión obligatoria.

Si bien al momento no está aprobada la Ley de Protección de Datos Personales, se debe considerar estos lineamientos para gestionar la información de clientes y consumidores y anticipar posibles requerimientos normativos que implementados luego puede ser costoso y complejo.

5

Relaciones con proveedores de tecnología:

Posiblemente las empresas realizaron adquisiciones de emergencia o cambiaron condiciones con proveedores existentes.

Estas nuevas condiciones deben siempre mantener niveles de calidad y servicio acorde a las necesidades de la compañía, por lo que se sugiere implementar procesos de monitoreo continuo para proveedores de servicios tecnológicos y apoyarse de auditorías y evaluaciones independientes que permitan conocer la madurez de los procesos, controles de TI y de seguridad del proveedor.