Highlights

Junio 2018

Presentamos los resultados del Global Entertainment & Media Outlook 2018-2022, incluyendo hallazgos globales, regionales y locales; así como una entrevista a Alexander García, director de Consultoría de Negocios, respecto a la importancia de contar con un sistema de ciberseguridad eficiente. Finalmente, algunas recomendaciones para llevar el uso de redes sociales corporativas a un nuevo nivel.

Global Entertainment & Media Outlook 2018-2022

¿Cómo crecerá la industria de entretenimiento en los próximos cinco años?

En tiempos en los que la tecnología y la información reinan, la confianza se ha convertido en un factor crítico para el éxito en los negocios, lo que podría resultar en un gran diferenciador para las industrias.

La información de nuestro reciente estudio ofrece una perspectiva única en tres de las principales tendencias que influyen en la estrategia de las industrias a nivel global: confianza, convergencia y conexiones. Empresas provenientes de diferentes rubros apuntan a modelos comerciales enfocados en relaciones integrales directas con el consumidor; y es esta convergencia la que genera competidores cada vez más fuertes, por la conexión que ya han establecido con sus clientes y otros stakeholders.

Principales hallazgos:

Acceso a internet

Los ingresos totales por acceso a internet en Perú pasarán de ***US$2,552*** millones en 2018 a ***US$3,593*** millones en 2022.

84% de esos ingresos corresponderán a dispositivos móviles.

Cine

Brasil será el país que más crezca en la región, hasta alcanzar ***$1.2*** MM al 2022.

Latinoamérica tendrá el menor crecimiento a nivel global: ***$3.1*** MM al 2022, frente a los ***$13.1*** MM de Norteamérica o los ***$24.5*** MM de Asia-Pacífico.

Videojuegos / e-sports

Ingresos totales para Latinoamérica al 2022: ***$3.7*** MM.

Publicidad en videojuegos crecerá en ***13.7%*** anual en la región.

Publicidad corporativa

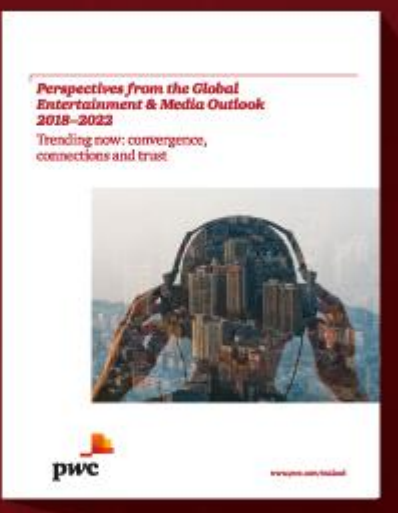
El mercado B2B latinoamericano es el más pequeño, con solo ***2.5%*** del ingreso global. Este es 6 veces menor al de Asia-Pacífico.

En Perú, crecerá a un ritmo aproximado de ***6.4%*** anual.

TV

La suscripción de TV en Latinoamérica crecerá ***1.3%*** anual hasta alcanzar ***$16.6*** MM al 2022.

En Perú el crecimiento será de ***1.4%*** hasta los ***$658*** M en el 2022.



Para más información sobre el estudio, clic aquí:
https://pwc.to/2HMrbIr

Entrevista PwC

Alexander García

Director de Consultoría de Negocios de PwC

La transformación tecnológica expone a las empresas a riesgos que pueden dañar su reputación y tener un impacto financiero. Una estrategia de ciberseguridad adecuada puede proteger los activos de la compañía y ayudar a prevenir o mitigar el impacto de un ataque

¿Cuál es la diferencia entre la ciberseguridad y la seguridad de la información?

La ciberseguridad incluye todas las estrategias, procesos, herramientas y personal experto que tienen las compañías para proteger sus activos tecnológicos y digitales. Estos los puedes encontrar en los servidores, en la nube, en los celulares o correos electrónicos utilizados por las empresas actualmente. La diferencia con la seguridad de la información radica en que esta abarca también activos no digitales, es decir, aquello que puedes encontrar en contratos, documentos confidenciales, recetas o historial médico, por ejemplo, que forma parte de información sensible de la compañía y que es de alta utilidad para los negocios.

¿Por qué es importante tener una estrategia de ciberseguridad y cómo el no tenerla puede dañar a las compañías?

Una estrategia de ciberseguridad es importante porque es la forma en que una organización decide proteger sus activos digitales, y representa la hoja de ruta por donde la compañía va a caminar para mejorar su nivel de madurez en cuanto a medidas de seguridad. Una empresa que no tenga una estrategia definida probablemente invierta en tecnologías que, de repente, no protejan los activos digitales que la compañía necesita o los más relevantes para su negocio. Asimismo, podría no abordar adecuadamente los riesgos a los cuales está expuesta y, por último, no tener los medios para contener y responder ante amenazas informáticas cuando estas afecten sus sistemas de información.

¿Qué características debe tener el profesional dedicado a la ciberseguridad?

Un experto de la ciberseguridad, contrario a lo que la gente piensa, no debe tener únicamente competencias técnicas sino también una alta capacidad para analizar, inquietud por investigar, ya sea ataques informáticos o

herramientas, y estar siempre actualizado. Debe sentir interés también por la parte estratégica, porque no solamente se trata de implementar soluciones tecnológicas sino tratar de adecuarlas a la industria en la cual se mueve la compañía. Sin embargo, es importante que las organizaciones consideren que los ciberataques y la ciberseguridad no solo son responsabilidad del área de tecnología o de seguridad de la información. La forma como la empresa debe protegerse de estos ataques comienza en la alta dirección y gerencia de las compañías, donde se debe definir los lineamientos, estrategias y presupuesto para que la organización en su conjunto, en sus diversas áreas operativas, pueda implementar y desarrollar las medidas adecuadas para evitar o prevenir el cibercrimen que puede perjudicar no solo el lado financiero sino también el reputacional.

Según el Estudio Global de Delitos Económicos y Fraude 2018 de PwC, más del 30% de organizaciones señala haber sido víctima de un delito cibernético. ¿Cuáles son las técnicas de cibercrimen más usadas?

Los dos tipos de cibercrimen que más afectan a las empresas son el *phishing* y el *ransomware*. El primero es un ataque informático mediante el cual el hacker se hace pasar por otra persona para obtener o robar información confidencial. La segunda técnica ha golpeado mucho el año pasado en diversos sectores de negocio. En ese caso, se utiliza un programa malicioso llamado *malware*, que se infiltra en las redes de las empresas e inutiliza y encripta los sistemas de información. Luego, para desbloquearlos, el atacante pide un rescate, por lo general en criptomonedas, por ser un método de pago muy difícil de rastrear.

¿Cómo empezar a desarrollar un sistema de ciberseguridad?

Se debe empezar identificando cuáles son los activos tecnológicos más relevantes para la operación de la empresa. Por ejemplo, en el caso de una clínica, un activo sería la información de los pacientes. Luego, se evalúa si las medidas de seguridad implementadas son lo suficientemente robustas para cubrir o mitigar la mayor cantidad de riesgos posibles de un ciberataque o robo de información.

Finalmente, una estrategia de ciberseguridad también debe abordar el aspecto de contención y respuesta, porque ninguna compañía es infalible ante estas situaciones. Se debe estar preparado para ser atacado y también para responder al ataque, contenerlo y recuperar las operaciones.

¿Qué otras medidas están adoptando las empresas para responder ante posibles ataques cibernéticos?

Una de las tendencias actuales son los ciberseguros. Estas pólizas protegen a las compañías frente a ataques informáticos, no solo mitigando cualquier riesgo de pérdida financiera, robo de información o la penalidad de algún regulador, sino también permitiendo afrontar los gastos que implica una situación de este tipo. Es decir, si necesito recurrir a un servicio de investigación de cómputo forense para que me ayude a determinar cuál fue la causa del ciberataque, determinar responsables y potencialmente hacer juicios a los que se definan como culpables.
Los ciberseguros, a nivel global, están siendo adoptados en un 40% a 50% en diferentes industrias, y es una medida que las empresas toman para poder proteger aquellos aspectos que, por la naturaleza del riesgo, son difíciles de prevenir de manera proactiva.

Contacto:
alexander.garcia@pe.pwc.com

Digital Pulse

¿Qué tan efectivas son las redes sociales de tu empresa?

El uso corporativo de las redes sociales aún no alcanza un buen nivel de desarrollo. Algunas compañías miden su efectividad basándose solo en cuántos *likes* tuvieron sus publicaciones. Sin embargo, los beneficios del *social media,* en un nivel más avanzado, no solo impactan en los esfuerzos de marketing, sino en todo el negocio.

Puedes leer la versión completa de este artículo en Digital Pulse de PwC:
https://pwc.to/2txjOAm

Conoce nuestro blog desafios.pwc.pe

Incubando ideas desde PwC Perú

Aquí encontrarás más articulos sobre la visión de nuestros especialistas en relación con las tendencias de los negocios en nuestro país y el mundo, además de soluciones prácticas a los principales desafíos de nuestros clientes.

Para mayor información visita: ***www.desafios.pwc.pe***
