MINISTERIO DE COMUNICACIONES

Boletín *Novedades TIC*

Junio *2020*

Contenido

Sistema de Vigilancia Tecnológica

Ministerio de Comunicaciones

#QUEDATEENCASA #CUBASALVA

SEGURIDAD INFORMATICA

1. LA "NUEVA NORMALIDAD" EXIGE GARANTIZAR LA SEGURIDAD DE LA INFRAESTRUCTURA FÍSICA

Fecha: 24/06/2020

En medio de los cambios que ha traído el teletrabajo, los directores de TI y los líderes de innovación se enfrentan al reto de asegurar la continuidad de la operación con base en la adecuada gestión de los recursos tecnológicos.

¿Qué hacer para que los colaboradores tengan acceso a los entornos de red y a las aplicaciones desde sus casas? ¿Cómo mantener los niveles de seguridad controlados? ¿Cómo preservar la buena gestión de TI ahora que se combinarán las modalidades de trabajo: tanto remoto, como en las oficinas?

"A raíz del COVID-19, las organizaciones han tenido que dar paso a escenarios no controlados. Las políticas de seguridad informática se han flexibilizado y los riesgos de seguridad cibernética han aumentado", explica Vladimir Linares, Technical Systems Engineeer de Panduit, compañía que opera en 112 países y que se especializa en soluciones avanzadas de infraestructura física, eléctrica y de red para entornos empresariales.

En su concepto, "la nueva normalidad, en la que los empleados combinarán tiempos de trabajo en casa con el regreso paulatino a las oficinas, exige mayores niveles de seguridad. Por tal razón, es necesario que las empresas adopten, entre otras las siguientes medidas: adecuación de sistemas de cableado mucho más inteligentes, configuración de nuevas políticas de seguridad, mayor monitoreo y sistemas avanzados de alarmas, que logren advertir a tiempo posibles ataques o situaciones anormales".

Panduit responde a estas necesidades a través de un conjunto de herramientas que ofrecen soporte proactivo de seguridad en redes. La primera de ellas es Smartzone Connectivity, sistema inteligente de monitoreo de red. Incluye entre sus componentes: panel de conexiones, panel de administración, cables de conexión y bandeja de fibra, así como alarmas en tiempo real y trazabilidad de las conexiones.

"Con esta solución se pueden enfrentar situaciones relevantes de conectividad, continuidad del negocio y seguridad de los datos. Incluye configuración de políticas de seguridad por puerto, monitoreo y seguridad; información en tiempo real sobre la conectividad de la red; monitoreo y alertas de cualquier cambio o alteración; opción de interconexión y conexión cruzada; lo mismo que mapeo de cables y rastreo visual", afirma Linares.

En cuanto a desafíos como el acceso de intrusos a las redes, uno de los más frecuentes en la actualidad por las vulnerabilidades creadas, Linares resalta el valor que ofrecen productos de seguridad física como SmartKeeper, que ofrece mecanismos de bloqueo para evitar el acceso no autorizado a puertos abiertos, agregando una capa física al sistema de seguridad que ya existe.

"Funciona como una llave maestra que controla múltiples dispositivos para bloquear una variedad de puertos abiertos, lo que reduce el riesgo de daños intencionales o no intencionales. Ahorrando tiempo y dinero a las organizaciones asociados con violaciones de datos, tiempos de inactividad de la red y reparación de la infraestructura".

De igual manera se destaca IntraVUE Edge, herramienta que proporciona capacidades de diagnóstico de la red, además de visualización y monitoreo en tiempo real mejorando el tiempo de actividad de la infraestructura. Los responsables de las áreas IT pueden realizar mapas de conexiones, asegurar accesos remotos de más de 1.000 dispositivos y generar alertas y monitoreos con envíos por SMS o correo electrónico.

"Estamos en una época llena de desafíos. Es claro que debemos reimaginarnos muchas cosas y el tema de la seguridad de la infraestructura debe ser un punto clave en el retorno y el aseguramiento de las operaciones de las empresas. Panduit es el aliado ideal que ayuda a las organizaciones a enfrentar estos nuevos retos con inteligencia", puntualiza Vladimir Linares, Technical Systems Engineeer de Panduit.

Disponible en:
https://www.tynmagazine.com/la-nueva-normalidad-exige-garantizar-la-seguridad-de-la-infraestructura-fisica/

2. TELETRABAJO Y CIBERSEGURIDAD, UNA NECESIDAD PRIORITARIA

Fecha: 22/06/2020

Según datos del INE solo el 27% de las compañías había experimentado el teletrabajo antes de la llegada de la pandemia de coronavirus, ahora ese porcentaje ha crecido exponencialmente, complicando también las medidas de seguridad en las compañías.

La pandemia del Covid-19 revolucionó el mundo tal y como lo conocíamos en cuestión de días y para poder mantenerse, la mayoría de las empresas se vieron obligadas a organizar sus equipos y sistemas y mandar a sus empleados a trabajar desde casa. Esto, ha supuesto un reto importante desde muchos frentes, también desde el frente de la seguridad.

Según datos del Instituto Nacional de Estadística (INE), solo el 27% de las compañías había experimentado el teletrabajo antes de la llegada de la pandemia de coronavirus. Solo un 7% de la población trabajaba en remoto de forma esporádica y e 4% lo hacía de manera continua. Sin embargo, de manera repentina, se nos ha abierto un nuevo escenario en el que la tendencia es masiva debido a que las organizaciones se han visto obligadas a instalar esta fórmula para dar continuidad a sus negocios. Ante esta falta de preparación general, los riesgos han aumentado, y las propias empresas han iniciado una carrera por asegurar sus sistemas en remoto y aprovechar, de paso, para prepararse de cara un futuro en el que estas estadísticas aumentarán exponencialmente.

Por otra parte, las amenazas han crecido; los cibercriminales buscan sacar rédito de esta crisis y los empleados se ven amenazados por multitud de vectores a los

que en muchos casos no saben como hacer frente. Desde el phishing hasta llegar al ransomware, el ramillete de ataques es muy numeroso. Por ello, los trabajadores, además de necesitar herramientas técnicas de ciberseguridad, buscan guías que les capaciten para tener bajo control este nuevo fenómeno.

Para tratar y analizar la situación respecto a la seguridad en tiempos donde el teletrabajo está creciendo y expandiéndose, la publicación CSO, de IDG Communications, ha celebrado una mesa redonda en la que agentes destacados de la industria han dado a conocer la situación en diferentes sectores.

La complejidad no ha sido solo montar las tecnologías, sino también habilitar los mecanismos legales para que lo que es el trabajo estuviera cubierto

Estos los últimos tres meses, como comentaba Lucía Galache, CISO de Unísono, "han sido una locura", pues, como ha sido su caso, han tenido que adaptar el trabajo remoto para más de 7000 empleados en España y el extranjero. "Hasta ahora no hacíamos teletrabajo concretamente por temas de seguridad de la información, pero ahora no nos ha quedado más remedio".

Ante la cuestión de si dar prioridad a la continuidad de negocio o a la seguridad, tanto Galache, como otros asistentes coinciden en que se ha primado la continuidad del negocio y ya después se ha empezado a gestionar los temas de la ciberseguridad. "En Unísono hemos intentado ir en paralelo, la continuidad del negocio es fundamental y fue la primera alarma, pero hemos idoacompañando todos los procesos de seguridad".

Hay que diferenciar entre el teletrabajo y la situación en la que se han visto inmersas casi todas las compañías de "trabajar desde casa"

Ha habido casos como el del Servicio Madrileño de Salud, donde, como ha expuesto su CISO, Ángel Luis Sánchez, ya conocían el terreno pues vivieron una prealarma con la Gripe A. "Estábamos preparados en cuanto a la parte tecnológica pero es cierto que una parte es tener eso y otra poder gestionar la organización. Ya trabajábamos con tecnologías como las VPN, Zoom, etc pero a una escala muy baja y esta situación ha requerido una inmersión completa". Por otro lado, Sánchez aclara que la complejidad no ha sido solo montar las tecnologías, sino también habilitar los mecanismos legales para que lo que es el trabajo estuviera cubierto.

El hecho de teletrabajar, afecta directamente al perímetro de seguridad. "No tenemos control sobre las redes wifi que los empleados tienen en sus hogares o sobre los equipos particulares con los que también trabajan a veces y esto supone retos muy amplios" comentaba Miguel Monedero, director de seguridad de la información de Sothis.

En un contexto como este, Rafael Hernando, CISO de Cepsa ha planteado una cuestión cuanto menos interesante como es la realidad de que hay que diferenciar entre el teletrabajo y la situación en la que se han visto inmersas casi todas las compañías de "trabajar desde casa". Dos cuestiones que son bien diferentes.

"Para teletrabajar son necesarios unos procesos que en la mayoría de los casos no se han llevado a cabo y son importantes. Hoy por hoy los empleados no cuentan con los mismos servicios en sus oficinas que en sus hogares. Hemos dado un paso importante hacia la digitalización, pero esto aún no se puede considerar teletrabajo".

Disponible en:
https://cso.computerworld.es/cibercrimen/teletrabajo-y-ciberseguridad-una-necesidad-prioritaria

3. ¿CÓMO SABER LO QUE ES ADECUADO PARA CREAR UNA SÓLIDA CIBERDEFENSA?

Fecha: 22/06/2020

En organizaciones de todo el mundo se suele tener la idea equivocada de que adoptar un buen enfoque en seguridad mantendrá seguros los datos de negocio y alejados a los ciberdelincuentes. Pero ¿cómo saber lo que es apropiado y si será lo suficientemente bueno?

En organizaciones de todo el mundo se suele tener la idea equivocada de que adoptar un buen enfoque en seguridad mantendrá seguros los datos de negocio y alejados a los ciberdelincuentes. Pero ¿cómo saber lo que es apropiado y si será lo suficientemente bueno?

Las amenazas actuales se dirigen a personas y no a infraestructuras. Ante esta realidad, las soluciones y los controles técnicos siguen siendo cruciales para construir una fuerte ciberdefensa, pero son solo una parte de la amplia y sólida barrera que existe para frenar lo último en amenazas.

A través de enlaces maliciosos, compromiso de cuentas o ingeniería social, los ciberdelincuentes están centrando su atención en la que para muchas organizaciones es su última (y a menudo no muy bien preparada) línea de defensa: los empleados.

No importa lo robustos que sean los sistemas de una organización, solamente hace falta que un empleado haga clic para que los delincuentes estén dentro.

Es necesario un nuevo enfoque de seguridad ahora que el teletrabajo ha entrado a formar parte de la "nueva normalidad". Este enfoque debe situar a las personas en el centro de la ciberdefensa y asegurarse además de que no solo los empleados son capaces de detectar y disuadir los ataques, sino de que son conscientes de cuál es su función en la seguridad de las organizaciones.

El repunte de las amenazas BEC

Con millones de empleados trabajando desde casa fuera de los límites de la oficina en cuanto a protección, organizaciones de todo el mundo han visto cómo ha aumentado su superficie de ataque, dejándolas más expuestas que nunca a las ciberamenazas en plena crisis por el Covid-19.

Los ciberdelincuentes están al tanto de esta situación y no han perdido el tiempo en aprovechar la oportunidad. Incluso antes de que se declarara oficialmente la pandemia mundial, especialistas en inteligencia de amenazas detectaron grandes volúmenes de ataques de phishing relacionados con el coronavirus, desde mensajes que ofrecían una supuesta vacuna hasta los que solicitaban

datos para una base de datos falsa del gobierno. En estos momentos, con medidas de desescalada que varían según la región, se prevé una nueva adaptación de los ataques mediante señuelos sobre la reapertura de oficinas, entre otros temas.

Independientemente del señuelo que se utilice en un ataque por correo electrónico, el objetivo es el mismo: aprovecharse de la vulnerabilidad humana. Los ciberdelincuentes intentan engañar a los empleados de organizaciones, mediante ataques de ingeniería social, para robar credenciales o datos confidenciales, desviar pagos y transferir fondos de manera fraudulenta. No importa la técnica empleada, solo se necesita un clic para que un ciberataque tenga éxito.

Una de las amenazas por correo electrónico que se ha disparado en los últimos años son los ataques BEC (Compromiso de Correo Electrónico Empresarial). Su éxito se basa en dos simples razones: es un método que funciona y que, además, reporta ganancias. Tanto es así que el FBI emitió recientemente un comunicado en el que calculaba un coste de 26.000 millones de dólares desde 2016 en negocios de todo el mundo.

Bajo estas cifras se esconden empresas de todo el mundo que sufren las consecuencias. El año pasado la empresa subsidiaria Toyota Boshoku fue víctima de la mayor pérdida jamás registrada por un solo ataque. Un impostor se hizo pasar por un socio comercial y acabó convenciendo a la filial de hacer una transferencia por valor de 37 millones de dólares a una cuenta falsa. Por citar algún caso más reciente, Puerto Rico perdió más de 4 millones de dólares el pasado enero en tres ataques BEC diferentes dirigidos a agencias gubernamentales. Asimismo, en mayo, el fondo de inversión estatal Norfund, de Noruega, recibió un correo electrónico por parte de unos impostores a los que transfirieron 100 millones de coronas noruegas (aproximadamente unos 10 millones de dólares).

Construir hoy las defensas de mañana

En estas circunstancias tan excepcionales que estamos viviendo ha quedado de manifiesto que la ciberdefensa de las organizaciones se queda en nada cuando toca defenderse de ataques BEC. Con tantos empleados trabajando en remoto, y cada vez más dependientes del correo electrónico, se ha dejado al descubierto un punto débil importante, pero que las organizaciones no están abordando.

Las personas y el correo electrónico conforman la superficie de ataque preferida en la actualidad por los ciberdelincuentes, y la mayoría de las estrategias de ciberdefensa no contemplan esta realidad. A pesar de que más del 90% de las amenazas avanzadas proviene del correo electrónico, solo el 10% del gasto en ciberseguridad se centra en esta área.

Los que están en primera línea sufren también una falta de inversión similar. La mayoría de las organizaciones realiza menos de dos horas de formación en ciberseguridad al año, lo cual evidencia la falta de concienciación sobre amenazas entre los usuarios finales. Solamente el 66% de la fuerza laboral en el mundo sabe lo que es el phishing, mientras que el 31% está familiarizado con el ransomware. Esto es algo que debe cambiar. No podemos

esperar que las personas protejan a las organizaciones sin equiparlas con las herramientas y conocimientos necesarios para hacerlo.

Del mismo modo que los ciberdelincuentes han aprovechado esta oportunidad para perfeccionar sus ataques, también es el momento de que las organizaciones perfeccionen sus defensas. No se pueden crear estrategias de ciberseguridad sobre principios del pasado. Estas deben reflejar el panorama actual de amenazas y estar preparadas para los ataques de mañana.

La falta de concienciación y formación de los empleados está generando una brecha de seguridad en muchas ciberdefensas, algo en lo que las organizaciones deberían trabajar.

Las personas, en el centro de la defensa

Los ataques por correo electrónico ya estaban causando verdaderos estragos antes de la pandemia del coronavirus y seguirán en la misma línea por mucho tiempo. Sin embargo, la adopción masiva del teletrabajo de manera forzada ha servido de oportunidad para ver cuáles son los ataques más comunes a los que se enfrentan las organizaciones, así como los controles que deben ponerse en marcha para defenderse de ellos. Es un ejercicio que debería de haberse hecho hace tiempo.

La seguridad de la red y de los endpoints continúa como el principal foco de atención de los equipos de seguridad. Aunque están lejos de ser el objetivo número uno de los atacantes, no por ello deben dejar de ser motivo de preocupación para las organizaciones.

Defender el perímetro es una práctica obsoleta. No hay un perímetro que defender. Los empleados están en movimiento, acceden a los datos de la empresa desde cualquier lugar y a través de distintos dispositivos, redes y plataformas fuera del entorno corporativo tradicional. Las personas son ahora el blanco de la mayoría de los ciberataques, por lo que es lógico que vayan en el centro de la ciberdefensa.

Detectar y disuadir las amenazas comunes requiere una fuerza laboral vigilante y bien informada, que sea muy consciente de su papel a la hora de mantener a su organización segura, así como estar al tanto de cuáles son las consecuencias de no hacerlo. Esto pasa por una formación continua y adaptada de los empleados en materia de ciberseguridad.

Una capacitación que vaya más allá de concienciar de forma general acerca de las amenazas comunes y que lleve a los usuarios finales a comprender cómo su comportamiento puede marcar la diferencia entre un intento de ataque y un ataque exitoso.

Una buena ciberdefensa no es suficiente para protegerse frente al panorama de amenazas tan dinámico que existe hoy en día, como así pueden comprobar organizaciones de todo el mundo. El objetivo principal de estos ataques es hacer daño a los negocios; y si la defensa no está en primera línea, habrá un único ganador.

Disponible en:
https://cso.computerworld.es/tendencias/como-saber-lo-que-es-adecuado-para-crear-una-solida-ciberdefensa

4. LA IA, ESENCIAL PARA FRENAR LA CIBERDELINCUENCIA

Fecha: 13/06/2020

El aumento de la automatización de los ataques y su creciente sofisticación hace que la inteligencia artificial sea cada vez más necesaria para combatir la ciberdelincuencia.

Las noticias acerca del aumento del número de ciberataques, de su impacto, de su automatización y de su sofisticación no dejan de sucederse. Y a la par que el mundo de la ciberdelincuencia evoluciona, también lo hace la ciberseguridad.Por ejemplo, hace algunos meses hablábamos del uso de técnicas de deception para engañar a los atacantes. Por otro lado, la utilización de inteligencia artificial (IA) para hacer frente a los ciberdelincuentes es una de las soluciones que más interés despierta.Según una encuesta realizada por Delta Computing a 130 responsables de TI, la IA se muestra como una herramienta indispensable para combatir la ciberdelincuencia, tal y como recoge Computing. En una escala del 1 al 7, el nivel promedio de acuerdo con la afirmación de que “la seguridad cibernética mejorada por IA es necesaria para operar en el panorama de amenazas actual” es de 5,5 puntos.Por tanto, los responsables de TI se muestran claramente a favor de la implementación de la IA en el ámbito de la ciberseguridad, debido a la creciente automatización por parte de los atacantes. No obstante, consideran que esta tecnología es insuficiente por sí sola, por lo que debe sumarse a las defensas existentes, a las que no puede reemplazar.

En este sentido, algunos de los consultados remarcan que las mejoras en el campo de la ciberseguridad suelen ser aditivas, de forma que el uso de nuevas herramientas rara vez sustituye a las anteriores, sino que las complementa. Sin embargo, el coste que supone el desarrollo e implementación de algunas soluciones de seguridad mejoradas por IA hace que no siempre sea posible mantener el resto de protecciones. Así pues, la mayoría de los responsables de TI encuestados se muestra de acuerdo en que una mayor automatización es esencial, especialmente cuando hablamos de defensas de red, correo electrónico y end-point. No obstante, reconocen que las dificultades para medir la efectividad de las soluciones mejoradas por IA, la novedoso de este mercado y los altos costes que tiene estas herramientas hacen que sea complicado justificarlas en términos de ROI, por lo que no es fácil defenderlas ante el director financiero de la compañía.

En cuanto a los argumentos para la incorporación de herramientas de ciberseguridad mejoradas, destacan la necesidad de adelantarse al panorama de amenazas, la minimización del riesgo corporativo y el alivio de la carga de TI. De hecho, una de las mayores promesas de la IA es precisamente su potencial para reducir la cantidad de alertas y de procesamiento manual. Sin embargo, la mayoría de los consultados afirmaron que aún se mostrarían reacios a aumentar los niveles de autonomía. De este modo, parece que la cesión de la toma de decisiones a las máquinas tendrá un enfoque gradual.

Disponible en:
https://www.silicon.es/ia-esencial-frenar-ciberdelincuencia-2416143

INTELIGENCIA ARTIFICIAL

1. LA INTELIGENCIA ARTIFICIAL DE HUAWEI AHORA MÁS CERCA QUE NUNCA DEL USUARIO

Fecha: 24/06/2020

HUAWEI ha desarrollado los sistemas de inteligencia artificial más avanzados y los ha puesto al servicio de las personas. Ahora toda esa tecnología llega a los dispositivos de HUAWEI en forma de asistente personal que te hace la vida un poco más fácil.

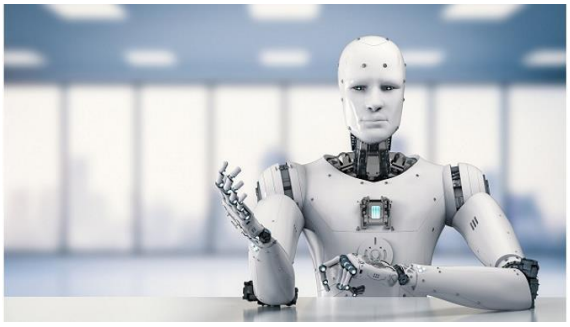
Gracias a las altas prestaciones de sus móviles y tabletas, ahora todos los usuarios pueden beneficiarse de esa inteligencia artificial integrada en su dispositivo móvil para hacer más eficiente su uso.

El Asistente de HUAWEI aprende de tus hábitos y rutinas mostrándote la información que necesitas justo en el momento adecuado, ayudándote en tu día a día y mejorando la experiencia de uso de tu dispositivo. Además, ahora mismo tienen una campaña activa con la que podrás ganar un móvil P40 Pro si habilitas estos servicios en tu dispositivo.

“TODAY es la apuesta de HUAWEI para dar a sus usuarios toda la información de valor disponible de la forma más rápida y más fácil posible. La actualización constante de sus contenidos y la alta capacidad de personalización de los mismos harán de este servicio uno de los favoritos de nuestros usuarios” explicaba Jaime Gonzalo, VP de HUAWEI Mobile Services Europa en un comunicado de la compañía.

Este Asistente utiliza la inteligencia artificial integrada en tu dispositivo para mostrar los datos de monitorización de tu actividad y muestra contenido dinámico con la información que más te interesa, justo en el momento que más la necesitas.

¿Tienes una reunión o tienes que viajar? Asistente HUAWEI te muestra a información más interesante relacionada con los eventos de tu calendario. En resumen, todo lo que necesitas para hacerte la vida más fácil.



Este Asistente ya está integrado en aquellos modelos que tienen instalado el sistema operativo EMUI 10.0 o posteriores como los nuevos móviles de la serie P40, pero también puedes beneficiarte de las ventajas de este asistente instalándolo en tu dispositivo HUAWEI si está actualizado a EMUI 9.0. Esto incluye series anteriores como los P20, P30 y toda la serie Mate 20.

Basta con acceder a la página del Asistente de HUAWEI y descargar el archivo de instalación APK para instalarlo en tu dispositivo. Además de experimentar el Asistente Personal en tu dispositivo, podrás ganar un móvil P40 Pro.

Después, solo tienes que activarlo desde el apartado Pantalla principal y fondo de pantalla del menú Ajustes de tu dispositivo. En este apartado, toca sobre la opción Ajustes de la pantalla principal y ahí encontrarás el interruptor que activa el Asistente de HUAWEI.

Desde ese momento, solo necesitas deslizar a la derecha la pantalla de inicio de tu dispositivo HUAWEI para acceder a una información dinámica que irá

cambiando a lo largo del día en función de tu actividad diaria ya que no se trata de un simple agregador de contenido, sino que aprende de tus hábitos de uso para mostrarte información útil en cada momento.

Celia, un asistente personal por voz con nombre propio

El Asistente de HUAWEI es un sistema de inteligencia artificial puesto al servicio de los usuarios para mejorar la experiencia de uso de los dispositivos, acercando la información al usuario de forma sencilla.

Sin embargo, la inteligencia artificial de HUAWEI avanza a pasos agigantados y este Asistente de HUAWEI cuenta con un complemento muy interesante con el que ni siquiera tendrás que tocar la pantalla de tu dispositivo.

Hablamos de Celia, un asistente por voz que utiliza AI Voice de HUAWEI para interactuar con el usuario mediante comandos de voz naturales. Basta con activar Celia mediante el comando "Hey Celia" y solicitar la información que necesitas, y Celia la mostrará en pantalla de forma inmediata.

Disponible en :
https://computerhoy.com/patrocinado/tecnologia/inteligencia-artificial-huawei-ahora-cerca-nunca-usuario-661287

2. QUALCOMM ROBOTICS RB5, PRIMERA PLATAFORMA DE ROBÓTICA QUE AÚNA 5G E INTELIGENCIA ARTIFICIAL

Fecha: 17/06/2020

Qualcomm Technologies evoluciona su tecnología para el mundo de la robótica y pasa de la plataforma Qualcomm Robotics RB3, que vio la luz el año pasado, a la plataforma Qualcomm Robotics RB5.

Esta evolución no se limita a un mero cambio de número. La RB5 es la primera solución de su clase que aúna la experiencia de Qualcomm en conectividad 5G e inteligencia artificial. Esta unión de fuerzas le permite ofrecer una solución más poderosa a desarrolladores y fabricantes para que avancen en la nueva generación de robots y drones de alto cómputo y baja potencia.

Qualcomm está pensando con su nueva plataforma tanto en máquinas para empresas, incluyendo los sectores industrial y de defensa, como en aquellas otras destinadas al consumidor, "más potentes, seguras e inteligentes que nunca".

Así las define Dev Singh, director sénior de desarrollo de negocio y responsable de robótica autónoma, drones y máquinas inteligentes en la compañía norteamericana, que busca "acelerar el crecimiento en una amplia gama de segmentos de robótica, como vehículos de guiado automático" o AGV, "robots móviles autónomos" o AMR, "drones y robots de entrega", así como "robots de inventario, industriales y colaborativos".

Qualcomm Robotics RB5 se compone de un amplio conjunto de hardware, software y herramientas de desarrollo. Su kit de desarrollo defiende como rasgos clave la personalización y la flexibilidad.

También apuesta por la seguridad. Su unidad SPU de procesamiento seguro incluye, entre otras garantías, aceleradores de cifrado, protección contra malware y autenticación biométrica, incluyendo reconocimiento de huella digital, iris cara y voz. A mayores, cuenta con certificación FIPS 140-2.

El procesador QRB5165 de la nueva plataforma de Qualcomm ofrece arquitectura informática heterogénea y la quinta generación del motor de inteligencia artificial de Qualcomm, con rendimiento de 15 TOPS para ejecutar cargas de trabajo complejas. Este chip integra una CPU Qualcomm Kryo 585 de ochos núcleos, GPU Qualcomm Adreno 650 y múltiples DSPs (cómputo, audio y sensor) e ISPs con soporte para siete cámaras concurrentes.

Aprovecha las capacidades del Hexagon Tensor Accelerator y de un motor de visión por ordenador dedicado para optimizar el análisis de vídeo.

Esa capaz de grabar vídeo 8K a 30 FPS y capturar fotos de 200 MP, además de vídeo 4K HDR a 120 FPS y fotos de 64 MP con retraso cero del obturador.

La nueva plataforma de Qualcomm es compatible con software como Linux, Ubuntu y Robot Operating System 2.0, así como drivers preintegrados para varias cámaras, sensores y conectividad 5G. También soporta OpenCL, OpenGL y OpenCV e Intel RealSense Depth Camera D435i y Panasonic TOF Camera.

En cuanto a la conectividad, puede trabajar con la tecnología 5G y la generación anterior, 4G. Y admite WiFi de largo alcance, WiFi 6 (802.11ax) y Bluetooth 5.1.

Para posibilitar una generación más potente de innovaciones en robótica, Qualcomm se ha asociado con TDK para mejorar las capacidades de Qualcomm Robotics RB5. Por ejemplo, TDK ha añadido tecnologías de sensor para aplicaciones robóticas mejoradas.

Son muchas las empresas que ya han mostrado su apoyo a Qualcomm, incluyendo una veintena de early adopters que han evaluado la plataforma, entre los que se cuentan gigantes tecnológicos como AWS, Intel y LG. Además, unas 30 compañías están desarrollando hardware y software para habilitar aplicaciones de robótica, como Canonical.

Se espera que los productos comerciales basados en Qualcomm Robotics RB5 vayan llegando al mercado a lo largo de este 2020.

Disponible en :
https://www.silicon.es/a-fondo-qualcomm-robotics-rb5-primera-plataforma-de-robotica-que-auna-5g-e-inteligencia-artificial-2416288

USO SOCIAL DE LAS TIC

1. DESAFÍOS DE SEGURIDAD Y TRANSFORMACIÓN DIGITAL QUE ENFRENTARÁN LAS EMPRESAS POST COVID-19

Fecha: 27/06/2020

Mientras algunos países todavía luchan por aplanar la curva de contagios del coronavirus y otros se preparan para reactivar su economía, todos por igual tendrán que enfrentar las consecuencias de la primera pandemia del siglo XXI. Una

de las más palpables, es la mayor demanda en los sistemas digitales y, por ende, presiones en los sistemas de ciberseguridad.

La implementación de operaciones remotas, una fuerza de trabajado dispersa y cambios en las cadenas de abastecimiento, han creado vulnerabilidades que antes no existían y que ponen a prueba los sistemas de seguridad informática.

"La Transformación Digital forzada que empresas han atravesado en los últimos meses, ha sido por la necesidad de llegar a su personal y sus usuarios de la mejor manera a sus manos. Como históricamente ha pasado en otras olas tecnológicas, la ciberseguridad a veces queda en segundo plano cuando la presión por lanzar servicios al público es mayor que nunca. Este es un momento crucial para que las empresas revisen todo lo que han hecho desde marzo, para revisar y asegurar cualquier brecha que sin intención se pudo haber abierto.", dice Eli Faskha, CEO de Soluciones Seguras.

Los cibercriminales han aprovechado esta situación. Google reportó que, durante la semana del 6 al 13 de abril, detectó más de 18 millones de correos electrónicos diarios de malware y phishing relacionados con estafas Covid-19.

En Panamá, las estafas Covid-19 también han aumentado. Los expertos de Soluciones Seguras han detectado que a partir de marzo se han incrementado los ataques de phishing y malware, usando el Coronavirus como un vector de ataque tratando de engañar al usuario con aplicaciones y noticias falsas.

Se han incrementado los ataques a los servicios que han implementado las empresas y organizaciones para habilitar el teletrabajo que son estos en la actualidad de misión crítica y que en algunos casos se lanzaron sin los análisis necesarios de seguridad.

Por esa razón, las empresas deberán hacer cambios significativos para enfrentar el futuro con más certeza. Entre ellos podemos destacar:

Detección de riesgo más profunda: Las empresas se deberán enfocar en su capacidad tecnológica a detectar amenazas, en formatos de trabajo remoto.

La comunicación y la respuesta de amenazas: Además de detectar las vulnerabilidades, los equipos de las corporaciones deberán crear planes para la respuesta a ataques y la comunicación a los equipos, que ahora son remotos, sobre todo en industrias que son críticas para el manejo de la pandemia, como la hospitalaria, dispositivos médicos, entre otras.

La seguridad en la cadena de abastecimiento: Además de pensar en la protección de los datos de los colaboradores, las empresas ampliarán sus acciones de seguridad a sus cadenas de abastecimiento, de manera que los encargados de seguridad deberán velar, no solo por los activos digitales, sino por la continuidad de toda la operación. El riesgo deberá manejarse de manera más integral.

Respaldo de los datos: En un entorno más digital, contar con un respaldo de los datos resiliente será vital, acompañado de

soluciones que permita una recuperación rápida de los datos, sin impacto al negocio.

Entrenamiento para el equipo de trabajo: El equipo de trabajo remoto debe estar preparado para actuar cuando hay alguna ciberamenaza. La capacitación a los colaboradores será un parte central de la agenda de las organizaciones en el futuro.

Con casi 20 años de experiencia en la gestión de seguridad de redes, aplicaciones y telecomunicaciones, Soluciones Seguras es la compañía líder en ciberseguridad en Centroamérica. Con un equipo de profesionales del más alto nivel, certificados por los fabricantes más reconocidos de la industria de seguridad, es el Centro Regional de Entrenamiento Autorizado Check Point número uno en la región. Cuenta con operaciones en Panamá, Costa Rica, Guatemala y El Salvador, y clientes en otros países de Latinoamérica.

Disponible en :
https://www.tynmagazine.com/desafios-de-seguridad-y-transformacion-digital-que-enfrentaran-las-empresas-post-covid-19/

2. TRANSFORMACIÓN DIGITAL: CAMINO SIN VUELTA EN UN MUNDO POST-PANDEMIA

Fecha: 18/06/2020

Antes el teletrabajo y las herramientas tecnológicas de redes, conectividad y seguridad eran una facilidad, ahora son una necesidad y los empleadores deben tener en cuenta que eso conlleva sin duda una inminente transformación digital en todos los aspectos. La conexión como herramienta de trabajo es mucho más importante de lo que era ayer, y la razón es justamente porque los clientes, las corporaciones y las empresas necesitan de él para obtener sus resultados.

Las empresas están buscando alternativas de conexión con tecnologías nuevas, y esto nos lleva a pensar eventualmente que la transformación digital se acelerará cada vez más durante y después del COVID-19.

La conectividad ha tenido una importancia relevante al despuntar un incremento en el tráfico de datos en contenido aproximadamente en un 60% más en México y Latinoamérica de lo que se veía antes de que esto sucediera. El consumo de entretenimiento en línea aumentó. El 70% del tráfico que transita se concentra en videos y audios streaming, contenido fotográfico o de juegos en línea, desde el uso de plataformas como Youtube, Netflix, HBOPlay, Facebook, Xbox, Play Station, Tinder, Snapchap y Spotify. El resto se distribuye en comercio electrónico, transacciones bancarias, mensajería instantánea, correos, conectividad VPN y tráfico a nubes.

Las compras en línea se dispararon. Según el Segundo Reporte sobre el Impacto del Covid-19 en Venta Online en México, recién lanzado por la Asociación Mexicana de Venta Online (AMVO), las razones más fuertes que los consumidores consideran para comprar en línea durante la pandemia han sido el no salir de casa (55%) y el evitar aglomeraciones en tiendas físicas (48%).

La telemedicina avanzó con pasos anchos. Las consultas online y el uso de dispositivos médicos como la video analítica y las cámaras con sensores térmicos ya son una realidad. También

hemos sido testigos de un proceso de digitalización sin precedentes en la educación. Estudiantes de todas las edades, desde el nivel básico al superior, sus responsables y maestros tuvieron que adaptarse rápidamente a la enseñanza en línea.

En el ámbito laboral,el internet tiene una relevancia fundamental, ya que laspersonas y sus herramientas de trabajo necesitan conectarse a través de la red. Se requiere que las empresas tengan tecnología definida para poder trabajar, sin dejar de lado también la ciberseguridad de los dispositivos que usen los empleados.

Hablamos de teletrabajo, conectividad y seguridad para poder sobrevivir esta pandemia, lo que significa adaptación y transformación digitalcomo una prioridad.

Ahora, ¿acaso el tejido empresarial de México estuvo preparado para esta crisis sanitaria?

La respuesta es que no lo estuvo del todo, pero esta emergencia sí ha provocado reflexiones y, más que eso, corroborado que, sin el uso de la tecnología, es imposible garantizar la continuidad de los negocios. En este sentido, entre las respuestas concretas y rápidas que vimos de parte de las empresas, podemos destacar:

Incremento del ancho de banda, que ha garantizado a sus empleados una buena conexión para hacer uso de videollamadas con frecuencia, acceder con facilidad a correos, entre otros servicios.

Adopción de soluciones en la nube para brindar movilidad, menos costos con infraestructura y actualizaciones en tiempo real.

Uso de VPN (Red privada virtual, por su sigla en inglés), una tecnología de red de ordenadores que garantiza la extensión segura de la red de área local (LAN) sobre una red pública o no controlada con internet.

Adopción de soluciones de CDN (red de distribución de contenido, por su sigla en inglés) para una entrega de los contenidos digitales y videos de alto rendimiento, con velocidad y seguridad.

Pero la transformación digital no solo se resume al tráfico de datos y herramientas tecnológicas, es un cambio cultural y de hábitos. Sin duda la “nueva normalidad”, será un reto y una oportunidad de adaptación personal y corporativa, tanto en México y como en el mundo.

Cuando la emergencia sanitaria termine, visualizamos un panorama en el que no se volverá al sistema de trabajo anterior. Las empresas deberán adaptarse a una nueva realidad, en la que la movilidad, el teletrabajo, la interconexión ya no serán diferenciadores, sino recursos indispensables para sobrevivir en un nuevo mercado y para atender a las demandas de una nueva generación de trabajadores y consumidores, profundamente impactados por esta experiencia.

Como lo mencionaba antes, es importante adaptarnos al cambio, aceptar esta transformación digital y hacer de esta necesidad una nueva y mejor forma de trabajo.

Disponible en :
http://cio.com.mx/transformacion-digital-camino-sin-vuelta-en-un-mundo-post-pandemia/

3. ¿CÓMO SERÁ EL MUNDO POST PANDEMIA?

Fecha: 09/06/2020

Pienso mucho en esto últimamente y creo que cuando volvamos a la "normalidad" será una normalidad diferente donde muchos aspectos cotidianos se verán atravesados por lo que nos tocó vivir a nivel global. Uno de esos aspectos, sin dudas, será el trabajo. Y el motivo es claro: en 2019, 62% de empresas de Latinoamérica no le permitían a sus empleados trabajar de forma remota (según el estudio El trabajador digital en 2019, Citrix). Vaya paradoja: ¡antes no podíamos elegir teletrabajar y ahora es obligatorio!

Pero, ¿cómo está resultando esa experiencia? Tal vez la respuesta a esta pregunta sea una mezcla de conformidad y disconformidad. El teletrabajo nos permite hoy estar seguros en nuestras casas conservando a la vez nuestro empleo. Nos está mostrando la maravilla de recuperar el tiempo que perdemos en el tránsito. Seguro hay empresas que estaban preparadas cultural y tecnológicamente para habilitar esta modalidad y sus empleados ya estaban preparados para teletrabajar de forma eficiente; pero aquellas que no, quizás estén creando contextos
de micromanagement abrumadores, sus empleados estén perdiendo productividad al encontrarse con tecnología que funciona más como un obstáculo que como una solución, y que encima puede exponer los datos a grandes riesgos.

Puede que haya personas pasando solas la cuarentena, que trabajan 24/7 con la excusa de mantenerse ocupados, pero que a la vez se sienten desgastados. O familias donde los padres además de trabajar tienen que atender en simultáneo a sus hijos, quedando con la sensación de no poder enfocarse 100% en nada. En este escenario, creo que no estamos solo teletrabajando. Estamos navegando una crisis mientras intentamos trabajar.

El teletrabajo es una modalidad con múltiples beneficios que tiene que realizarse en un contexto adecuado de trabajo. Tiene una curva de aprendizaje por parte de los empleados y requiere que los empleadores implementen un programa de calidad observando aspectos tecnológicos, culturales, de liderazgo y de recursos humanos.

Todo esto hace que sea un modelo exitoso. Pero en la actualidad, con tantos factores externos impactando en la productividad de las personas, la clave para las empresas será documentar qué funcionó bien al implementarlo y aquellos puntos a trabajar a futuro sin sacar conclusiones apresuradas. Por parte de los empleados, si el teletrabajo no cumplió sus expectativas probablemente tampoco es el momento adecuado para hacer una evaluación determinante sobre este modelo.

En este sentido, uno de los mayores aprendizajes que podremos llevarnos en el mundo corporativo será que todo espacio de trabajo tiene que buscar lograr el bienestar de los empleados. Y ese espacio debe impulsarlos y motivarlos para que puedan lograr su máximo potencial. Pero por sobre todo tiene que estar muy relacionado al poder ELEGIR. Ese poder que muchos no tenían antes y que no tenemos ahora. Ni los cubículos, ni los

espacios abiertos, ni el teletrabajo funcionan si los pensamos bajo el concepto de "lo mismo sirve para todos". En el futuro los empleados deberían poder elegir desde donde trabajar, incluso deberían poder alternar entre distintos espacios de trabajo según los objetivos que deban lograr. Y las empresas deberían asumir a la movilidad empresarial como una estrategia para crear un negocio dinámico y resiliente.

Esto necesitará que las empresas migren hacia una cultura que fomente la movilidad y genere confianza mutua. El liderazgo también deberá adaptarse porque en esta nueva realidad no será importante cuánto tiempo pasamos sentados frente a un computador, sino que tengamos objetivos claros y medibles a lograr. Y por supuesto, contar con tecnología que sea una aliada para lograr estos propósitos.

En definitiva, el camino hacia una experiencia de trabajo superior está marcado por la personalización y es hacia allí donde las empresas deben dirigirse ahora que finalmente se comprobó que el trabajo no puede ser un lugar al que vamos… tiene que ser una actividad que hacemos desde cualquier lugar.

-Juan Pablo Jiménez, vicepresidente de Citrix Latinoamérica y Caribe.

Disponible en :
http://cio.com.mx/como-sera-el-mundo-post-pandemia/

BANDA ANCHA

1. WI-FI 6, 5G Y LIFI: CARACTERÍSTICAS Y ANÁLISIS DE LAS CONEXIONES QUE ACELERARÁN EL INTERNET DEL FUTURO

Fecha: 21/06/2020

A continuación revisamos los modelos y tipos de redes que nos conectarán al internet del futuro, un mundo donde la velocidad reina. Aunque comercialmente no están del todo extendidos, ya cuentan con desarrollos y usos concretos.

Internet ha formado parte de nuestra vida como nunca antes. En el ámbito personal y laboral es la base de la gran mayoría de nuestras operaciones. Y como toda tecnología, evoluciona permanentemente; a veces, de forma sigilosa, y en otras ocasiones, con grandes cambios que repercuten directamente en la forma de conectarnos.

Precisamente respecto a los tipos de conexión y formas de acceder a la gran red, Fabian Erik Fink, Ingeniero de Aplicaciones Furukawa Electric LatAm, explica: "Sin duda, hoy la mejor conexión para acceder a Internet es por medio de la fibra óptica, pero si miramos nuestros dispositivos, no tenemos una conexión directa para la fibra óptica y necesitamos de conversores de medio. Es en este punto en que utilizamos las tecnologías inalámbricas y cableado en cobre".

Por eso, a continuación analizamos los modelos y tipos de redes que nos conectarán al internet del futuro en forma masiva, un mundo donde la velocidad reina. Aunque comercialmente no están del

todo extendidos, todos ya cuentan con desarrollos y usos concretos.

RED 5G

Quizás es la más fácil de asimilar para la mayoría de los usuarios, pues dice relación con la quinta generación de tecnologías móviles. Hemos hablado ampliamente de ellas, incluso de sus grados de avances y los respectivos obstáculos en América Latina.

Más allá de eso, 5G promete revolucionar nuestras vidas gracias a la transferencia de más datos y a mayores velocidades.

La actual red predominante, 4G, ofrece velocidades que rondan los 30 o 40 Mbps. Una buena conexión residencial hoy en día, por banda ancha, suele brindar entre 200 y 300 Mbps, con picos mayores en algunos casos sobre los 500Mbps. 5G, por su parte, se pronostica que alcance en promedio 575 megabits por segundo, es decir, 13 veces más rápida que la conexión móvil promedio actual. En cuanto a su potencial, asimismo, se calcula que puede llegar hasta 20 Gigabits por segundo.

Este potencial es tal que la red está llamada a ser la impulsora de una nueva revolución, pues a diferencia de las generaciones móviles anteriores, no se limitará a la navegación móvil desde dispositivos como los smartphones. 5G conectará también objetos que podrán comunicarse entre sí, facilitando así la era de Internet de las Cosas, con otras tendencias que confluyen como los vehículos autónomos o la telemedicina avanzada. La industria no será la misma.

Son muchísimos los alcances que se pueden hacer sobre esta prometedora red. Actualmente, según la GSMA, se reportan al menos 46 operadores en 24 mercados con redes comerciales 5G activas (cifras del informe al 30 de enero de 2020). Sin embargo, esta no es la única carretera de alta velocidad en la que transitaremos los próximos años.

Respecto a las proyecciones para 5G, basadas en avances técnicos, el representante de Furukawa resalta la necesidad de contar con redes de transmisión de fibras ópticas para garantizar el ancho de banda de la estación de radio base hacia las centrales de las operadoras. “Lo que vemos es que las grandes operadores tienen preparado un despliegue masivo de Fibra Óptica para que estén preparadas para 5G, por otro lado hay un movimiento de compartir la red de Fibra Óptica entre los operadores y esto puede acelerar el proceso de despliegue de la tecnología 5G”, agrega.

WI-FI 6

Cuando nos conectamos a wifi no acostumbramos poner atención a ciertos detalles. El anhelo por disfrutar de sus bondades opaca los aspectos técnicos de algo fundamental que ocurre de manera invisible. Estas conexiones son posibles gracias a ciertas definiciones ingenieriles eléctricas y electrónicas que se traducen, por ejemplo en el estándar 802.11ax, denominado Wi-Fi 6.

Se trata de la nueva generación del estándar de red de área local inalámbrica (WLAN) y llega como el sucesor del estándar Wi-Fi 5 (802.11ac), que usamos mayoritariamente hoy en día. Uno de los aspectos más destacados de esta evolución radica en que permitirá que los puntos de acceso admitan más clientes

(usuarios) en entornos densos y proporcionará una mejor experiencia para las redes LAN inalámbricas típicas.

Según nos cuenta Carlos González, ingeniero de sistemas en Cisco Chile, las principales diferencias tienen que ver específicamente con el cambio de paradigma respecto a la cantidad y calidad de conexiones que se están requiriendo hoy en día. Por eso, además, facilitará que aplicaciones de colaboración avanzadas, la transmisión de videos en 4K y 8K, realidad aumentada, realidad virtual y experiencias de inmersión, entre otros, tengan factibilidad.

El número promedio de dispositivos y conexiones por persona seguirá creciendo. Cisco estima que habrá cerca de 628 millones de puntos de acceso público a Wi-Fi para 2023, un aumento de cuatro veces respecto a 2018.

De igual forma, los puntos de acceso Wi-Fi 6 crecerán 13 veces entre 2020 y 2023 y serán el 11% de todos los puntos de acceso Wi-Fi públicos para 2023, a nivel global.

CÓMO SE RELACIONAN ENTRE ELLAS

Respecto a estas dos conexiones (5G y WiFi 6), la esencia es clara. Como señala Erik Fink, de Furukawa, hay una tendencia de redes internas a utilizar la tecnología Wi-Fi 6 y para redes externas la utilización de redes 5G. Por eso, como explica en palabras sencillas Carlos González, uno de los efectos más fuertes que va a tener WI-FI 6 es “equiparar la cancha” en relación a tecnologías wireless como 4G avanzado y 5G, pues estas serán mucho más veloces que los estándares actuales wifi.

Como sucede con la gran mayoría de los usuarios en América Latina y el mundo, priorizamos las conexiones wifi por sobre los datos móviles. Esto se evidencia cuando estamos en la calle y llegamos a nuestras oficinas u hogares. Sin embargo, con 5G funcionando, las velocidades y experiencias que nos ofrecerá haría que cambiáramos nuestro patrón y, en vez de activar el wifi en nuestra casa, mantendríamos nuestro plan de datos, que nos ofrecería conexiones mucho más rápidas que un wifi actual.

Precisamente para eso llega la actualización de WiFi 6. Como apunta el ingeniero de Cisco, esto será particularmente relevante para entornos corporativos, pues allí tienes redes y servicios internos propios de la compañía y existen ciertas normativas de seguridad que no resultan fáciles de aplicar a una red o escenario 5G. “Por decirlo de cierta manera, te van a obligar a usar el wifi para tener los servicios requeridos para trabajar”, comenta González.

Según adelanta Fabian Erik Fin, las redes 5G y WiFi 6 deberían tener un crecimiento fuerte en los próximos años, basadas en topologías con fibras ópticas. De igual forma, añade, en el próximo año podríamos tener una consolidación del WiFi 6 debido a la mayor cantidad de dispositivos compatibles y mejores precios.

UN NUEVO INVITADO: LIFI

Las dos redes ya mencionadas tendrán un rol protagónico en nuestro futuro cercano, pero no serán las únicas. Desde hace algunos años se ha venido hablando de una nueva conexión que ha generado grandes expectativas y llamado la atención

por lo novedoso del método. Se trata de LiFi, (Light Fidelity), una tecnología que permite el acceso a internet de banda ancha a través de la luz.

LiFi utiliza ondas de luz, en vez de las ondas de radio del wifi, para la transmisión de los datos y tiene como gran atributo un alto nivel de seguridad por su bidireccionalidad y con velocidades propias de una banda ancha.

Una de las compañías que ha desarrollado con mayor énfasis esta innovación es Signify (ex Philips Lighting), a través de su sistema denominado Trulifi. Permite superar la congestión permanente y creciente del espectro de radio (donde transitan señales como WiFi, 4G / 5G, Bluetooth, entre otras) y es ideal para zonas donde las radiofrecuencias no funcionan bien o no están permitidas.

Respecto al funcionamiento del sistema, según nos cuenta Eduardo Alvaro, Commercial Leader Professional South Latam de Signify, se modula la información sobre una fuente de iluminación y así se logra la transmisión de datos, “donde llega esa luz, llega la información”.

“Para conectarse a esta tecnología se requiere básicamente de un transmisor/receptor de datos a través de luz visible o infrarrojo, el cual se conecta a internet a través de un cable ethernet, y un dispositivo USB que hace las veces de transmisor/receptor y se conecta a una PC. El proceso de conexión es transparente al usuario final ya que con solo conectar el dispositivo USB a su PC y estar en línea de vista con el transmisor/receptor (puede ser una luminaria LiFi o un transmisor/receptor IR) ya se conecta a internet”, explica Alvaro.

Consultado respecto a la relación de esta solución con las otras conexiones, el representante de la compañía holandesa, sostiene que LiFi complemente a los otros sistemas, ya sean inalámbricos o cableados, aunque precisa que no ofrece una solución única para todos, pues dependerá del entorno y las necesidades del cliente. “Habrá aplicaciones donde LiFi reemplazará las tecnologías inalámbricas existentes. En otras aplicaciones, LiFi y, por ejemplo, WiFi funcionarán de la mano o se complementarán entre sí”.

Sin embargo, LiFi supone ciertas dudas y cuestionamientos para otros expertos. González, de Cisco, por ejemplo, nos cuenta que viene escuchando sobre esta innovación hace cuatro o cinco años, pero nunca ha visto un impacto muy fuerte o un desarrollo más acotado y concreto sobre esto. En ese sentido, apunta a que la misma tecnología wifi ha resuelto la mayoría de los problemas que tenía en coberturas con la aparición de repetidores o access point con mayor capacidad.

Respecto a Wi-Fi 6 y 5G, el vocero de Furukawa considera que trae nuevas oportunidades de servicios además del crecimiento que se registre en Internet de las Cosas, dispositivos de casa conectada, ciudades inteligentes y vehículos autónomos.

“Hoy con el COVID-19, dos de los principales negocios que ya está impulsando tanto el Wi-Fi 6 y el 5G es el Home Office y la Telemedicina, que hace un par de meses eran una tendência, mientras que ahora son una necesidad”, apunta Fabian Erik Fink. Y añade: “Hay otro negocio que también debe crecer: la

teleeducación, un servicio necesario como forma de distribución del conocimiento a los más remotos rincones del país".

Por su lado, Carlos González alude a las aplicaciones de próxima generación, aquellas que se vuelven tendencia y necesidad con los millones de usuarios y dispositivos conectados a la red y las velocidades y avances en conectividad a nivel de arquitectura. Estas aplicaciones tienen requisitos extremadamente complejos; son y se convertirán en una oportunidad de negocio muy importante, así como la creación de nuevos modelos de negocio.

Un ejemplo que cita el experto de Cisco hace referencia al análisis predictivo que emplea técnicas avanzada que aprovechan los datos para descubrir información en tiempo real y predecir eventos futuros. Esta tendencia puede transformar negocios y usarse en muchas soluciones como IoT industrial, con sensores para detectar fallas en los equipos, patrones climáticos, rotación de cultivos y varios otros impactos en la agricultura y la industria alimentaria.

Disponible en :
https://tecno.americaeconomia.com/articulos/wi-fi-6-5g-y-lifi-caracteristicas-y-analisis-de-las-conexiones-que-aceleraran-el-internet

2. SE LANZA LA PRIMERA COMPUTADORA CON TECNOLOGÍA 5G DEL MUNDO

Fecha: 18/06/2020

Qualcomm lanzó en junio de 2019, en conjunto con Lenovo, la primera PC 5G del mundo. "Project Limitless" fue el nombre del proyecto de colaboración tecnológica entre Qualcomm Technologies, Inc., líder en conectividad 5G, y Lenovo, líder en PC, para llevar la innovación al ecosistema de computadoras siempre conectadas.

Con el mundo cada vez más conectado y el uso de teléfonos inteligentes presente en casi todos los campos de la vida de los usuarios, las PC y las computadoras portátiles necesitaban reinventarse. Entre las principales ventajas de esta computadora portátil es que a diferencia de las clásicas tiene una batería que dura varios días y una conexión celular ultra rápida

Las PC siempre conectadas, mejor conocidas como ACPC, ya son una realidad mundial y se espera estén presentes en hogares y oficinas de la Argentina a futuro. Según la firma de investigación de mercado IDC, los envíos globales de PC ultradelgadas convertibles y desmontables están creciendo a un 12% anual.

Consciente del crecimiento de este mercado, Qualcomm desarrolla plataformas para computadoras como la familia Qualcomm Snapdragon 8cx, 8c y 7c, diseñadas para aumentar la productividad y el entretenimiento, gracias a la conectividad integrada y la batería de larga duración que ofrece la plataforma, todo en un formato elegante y moderno. La plataforma también ofrece experiencias transformadoras de 5G con el módem Snapdragon X55 5G, que también permite a los usuarios aprovechar la conectividad 4G LTE multi-gigabit.

La lista de los principales beneficios de las computadoras portátiles ACPC con Snapdragon incluye:

• Muy bajo consumo de energía, lo que permite que la batería dure días

• Conectividad celular extremadamente rápida. Para las plataformas 8cx y 8c, el módem ofrece velocidades máximas de descarga de hasta 2 Gbps

• Gráficos de alta calidad.

• Diseño extremadamente delgado y ligero.

• "Encendido instantáneo": posibilidad de activar inmediatamente el dispositivo de forma similar a un teléfono inteligente

• "Siempre encendido": permite que el dispositivo reciba correos electrónicos y notificaciones incluso cuando está en modo de suspensión

• Nuevas arquitecturas de IA para aplicaciones avanzadas.

Disponible en :
https://www.tynmagazine.com/se-lanza-la-primera-computadora-con-tecnologia-5g-del-mundo/

COMPUTACION EN LA NUBE

1. ¿SE VIENE LA SEGUNDA GUERRA DE LA NUBE?

Fecha: 21/06/2020

El mes pasado, cuando la popular empresa de videoconferencias Zoom anunció que firmaría un nuevo contrato de comutación en nube, no mencionó a sus proveedores actuales Amazon y Microsoft ni a Google. Zoom acudió a un titán de la tecnología al que muchos olvidaron que en plena competencia entre los tres grandes de la nube: Oracle.

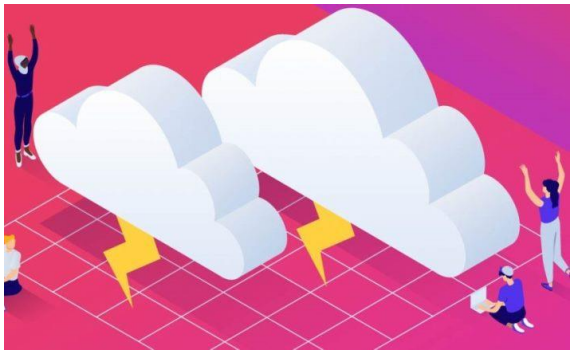
Semanas después, Oracle se anotó otra victoria al anunciar que le había robado otro cliente a Amazon, la plataforma de comunicaciones 8×8. Oracle aclaró cómo lo logró: precios 80% más bajos que Amazon Web Services, la muy rentable división de Amazon que lidera el mercado. "A diferencia de AWS, que te hace comprometer tus datos en el largo plazo con precios elevadísimos nosotros brindamos precios bajos todos los días", declaró la

No es la primera vez que Oracle le tira un palo a un competidor, pero ahora que la pandemia de COVID-19 lleva a las empresas a recortar gastos y a la gente a vivir y trabajar de manera remota en la nube, analistas de la industria afirman que las críticas de Oracle podrían formar parte de una nueva carrera para bajar precios entre los principales proveedores de nubes. Amazon ya recortó hasta 90% algunos precios; otros podrían imitarla. "La situación con la COVID y la asimilación de la adopción de nubes pondrán el acento sobre los precios", afirma Deepak Mohan, analista de la industria de la nube en IDC. "Es un nuevo tipo de guerra de precios".

Los servicios de computación en nube pasan desapercibidos por el público, pero hoy en día, lo más probable es que cualquier empresa grande, desde bancos, Netflix, las ligas deportivas y los fabricantes de gaseosas gasten millones de dólares (o incluso miles de millones en algunos contratos) para mantener sus redes, procesar la interacción con los

clientes y almacenar datos de manera remota.

Oracle se metió relativamente tarde en la lucha por dominar las nubes y tiene solo el 2% del mercado global, frente al 32% de Amazon, la líder de la industria, según datos de Canalys. Amazon está donde está por ser la pionera. Microsoft transformó a Azure en competidor en parte ofreciendo herramientas adecuadas para empresas a su extensa clientela. Por su parte, desde que entró al mercado en 2008, Google, que ocupa el tercer puesto, logró crearse un nicho con sus herramientas avanzadas de aprendizaje automático e inteligencia artificial.



Cuando anunció su contrato con Oracle, Zoom afirmó que planeaba procesar siete millones de gigabytes por día con la nube de Oracle. Con semejante volumen, se imponen los precios, y Oracle ya demostró su voluntad de bajarlos. 8×8, la otra empresa que dejó a AWS, está pagando un quinto de lo que le pagaba a Amazon por la salida de datos, afirmó Oracle.

En 2014, Google trató de promocionar su nube bajando hasta 85% los precios de algunos servicios, lo que obligó a AWS y a Microsoft a hacer descuentos. Ahora, parece que por lo menos Amazon hará lo mismo: bajó 40% los precios para los clientes de Sudamérica.

Hace poco, se reveló que Oracle había presentado una oferta junto a Microsoft para la licitación de un contrato de computación en nube de US$ 10.000 millones con el Pentágono, en la que competían con Amazon, pero se había retirado de la alianza cuando el Departamento de Defensa de EE.UU. señaló que le ofrecería el contrato a un solo proveedor. Microsoft ganó la licitación y Amazon apeló la decisión.

Oracle, que anunciaría sus ganancias el mes que viene, no especifica los ingresos obtenidos por su división de nube, pero como sus ingresos totales en el año pasado no superaron por mucho los US$ 35.000 millones que registró AWS en ventas en 2019, todavía le falta mucho para demostrar que puede competir con Amazon por el liderazgo en la nube.

Disponible en :
https://www.tynmagazine.com/se-viene-la-segunda-guerra-de-la-nube/ç

2. EL "ESTADO DE LA NUBE" EN ESTE DIFÍCIL AÑO 2020

Fecha: 09/06/2020

La nube se ha convertido en una metáfora de la propia informática moderna, donde todo es un servicio que puede conectarse y combinarse con otros para satisfacer un número infinito de necesidades de aplicación.

Tomemos incluso una aplicación de Software como Servicio (SaaS) relativamente simple como Slack: con sólo responder un formulario web, instantáneamente se obtiene la colaboración como un servicio. Pero a través de las API, se puede integrar Slack con docenas de otros servicios, desde Google Drive a MailChimp, pasando por Trello e incluso el principal competidor de Slack, Microsoft Teams. En otras palabras, unos pocos clics pueden ampliar drásticamente lo que Slack puede hacer.

Las posibilidades reales, sin embargo, emergen de las grandes nubes de IaaS:

Amazon Web Services, Microsoft Azure y la plataforma de nube de Google. Estos vastos ecosistemas contienen miles de servicios de nube más allá de la computación básica, el almacenamiento y las redes, y la capacidad de combinarlos en soluciones a medida ha cambiado para siempre la forma en que las empresas construyen aplicaciones.

En lugar de que los desarrolladores codifiquen cualquier cosa desde cero, recurren a las API para añadir, por ejemplo, servicios de aprendizaje automático, de bases de datos, de seguridad, de análisis o de cadenas de bloqueo. Si se usa algo de código abierto del servicio en la nube GitHub de Microsoft y se cuelga todo junto, se tendrá una solución empresarial viable que hace justo lo que se persigue en un tiempo récord.

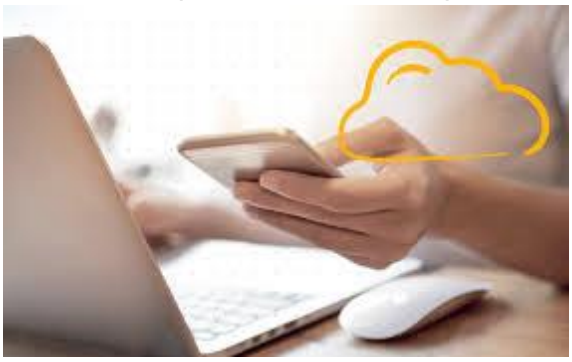
En este momento, en el que las empresas se enfrentan a una recesión económica (y en el que la mano de obra y el capital necesarios para poner en pie los servidores y licenciar el software pueden ser prohibitivos) parece inevitable un cambio acelerado a la nube.

La adopción de la nube vuelve a acelerarse

La Encuesta de Computación en la Nube 2020, recién publicada y elaborada por IDG tras consultar a 551 tomadores de decisión sobre compras de tecnología (todos involucrados en el proceso de compra de cloud), confirma que las empresas están haciendo planes agresivos en este modelo.

Según un 59% de los encuestados por IDG, sus organizaciones estarían en cloud en su mayoría o todas dentro de 18 meses. En la actualidad, el 32% de los presupuestos de sus organizaciones se destinan a cloud.

Y mientras que muchas de estas organizaciones han migrado las aplicaciones on-prem existentes a la plataforma de un proveedor de cloud computing, los encuestados estiman que el 46% de las aplicaciones fueron “construidas a propósito” para cloud, por lo que podrían aprovechar mejor la escalabilidad de este modelo y los modernos patrones de arquitectura.



En otra muestra de compromiso con la nube, el 67% dijo que han añadido nuevos roles y funciones de la nube, tales como los puestos de Arquitecto de la Nube, Administrador de Sistemas de la Nube, Arquitecto de Seguridad e Ingeniero de Desarrollo.

La computación sin servidores es quizás la expresión más pura del modelo en la nube como una serie interminable de servicios mixtos, incluso con infraestructura virtual en el espejo retrovisor. La nube no es simplemente un caballo de fuerza extra que se puede encender además de los estantes de los servidores on-prem. Es la arena en la que estamos construyendo el futuro de la informática.

Disponible en :
http://cio.com.mx/el-estado-de-la-nube-en-este-dificil-ano-2020/#more-130275

3. LOS 8 GRANDES RETOS DE LA GESTIÓN DE IDENTIDADES Y ACCESOS EN LA NUBE

Fecha: 01/06/2020

La “fatiga de contraseñas” o la “visibilidad de cumplimiento” son solo dos de los desafíos a los que se enfrentan las empresas, según Fujitsu.

La implementación de nuevas tecnologías trae aparejados tanto beneficios como retos que hay que superar. Una de esas tecnologías es la nube, cada vez más presente en las empresas y que supone un desafío considerable para los equipos de TI a la hora de gestionar identidades y accesos.

Según Fujitsu, son ocho los grandes retos de esta gestión, empezando por la “fatiga de contraseñas” asociada al alto número de aplicaciones que se acaban utilizando en la oficina. Cada aplicación tiene sus propios requisitos de contraseña y ciclos de caducidad, lo que a menudo termina con la frustración de unos usuarios que pasan mucho tiempo intentando recordar sus credenciales y reestableciéndolas. De ahí se pasa a la fatiga, que se materializa en el uso de contraseñas demasiado fáciles o repetidas y la anotación de estas en notas, con el peligro que supone. Con servicios IAM de gestión de identidades y accesos se puede ofrecer un inicio de sesión único basado en la nube y mayor seguridad.

En segundo lugar, Fujitsu habla del “proceso de aprovisionamiento automatizado de las aplicaciones”. Un buen servicio IAM en la nube permite añadir automáticamente nuevas aplicaciones, pero también facilita el aprovisionamiento de usuario automatizado en todas las aplicaciones in situ y las basadas en cloud, además de la opción de cancelar el acceso cuando un empleado deja de trabajar para la compañía. Ahora lo que ocurre en muchas empresas es que el acceso a las aplicaciones SaaS es concedido por el administrador de cada aplicación específica por separado en vez de por una sola persona de TI.

La “visibilidad de cumplimiento” o el “¿quién tiene acceso a qué?” es otra preocupación destacada. El servicio de IAM tiene que dejar que se establezcan derechos de acceso y proporcionar informes de cumplimiento centralizados para entender quién se está relacionando con los datos del negocio, cómo y dónde.

Otra clave son los directorios corporativos y la existencia de “directorios de usuarios aislados para cada aplicación”. Los recomendable en este caso es recurrir a la integración centralizada y lista para usar en el Directorio Activo Central o el directorio LDAP, sin necesidad de dispositivos locales ni modificaciones del cortafuegos.

Además, “gestionar el acceso a través de una multitud de navegadores y dispositivos” resulta fundamental, teniendo en cuenta que las aplicaciones cloud son accesibles desde cualquier equipo conectado a internet, incluidos los móviles.

En sexto lugar, hay que “mantener al día la integración de las aplicaciones” de distintos proveedores con políticas también diferentes. La solución de IAM debe mediar esa variedad de tecnologías y enfoques de manera transparente y simplificar la

llegada de nuevas aplicaciones al trabajo diario.

Como existen “diferentes modelos de administración para distintas aplicaciones”, un buen servicio IAM tiene que ofrecer a la parte de TI una administración central, seguridad, elaboración de informes y gestión de usuarios y accesos a través de las aplicaciones.

Por último, Fujitsu insiste en la “visión centralizada del uso de las aplicaciones”. Los modelos de suscripción mensual están reemplazando a la adquisición de licencias de software, para pagar por lo que se consume, pero esto entorpece la visión centralizada del uso. Por tanto, los gerentes necesitan acceso en tiempo real a informes para una toma de decisiones fundamentada.

Disponible en :
https://www.silicon.es/los-8-grandes-retos-de-la-gestion-de-identidades-y-accesos-en-la-nube-2415726