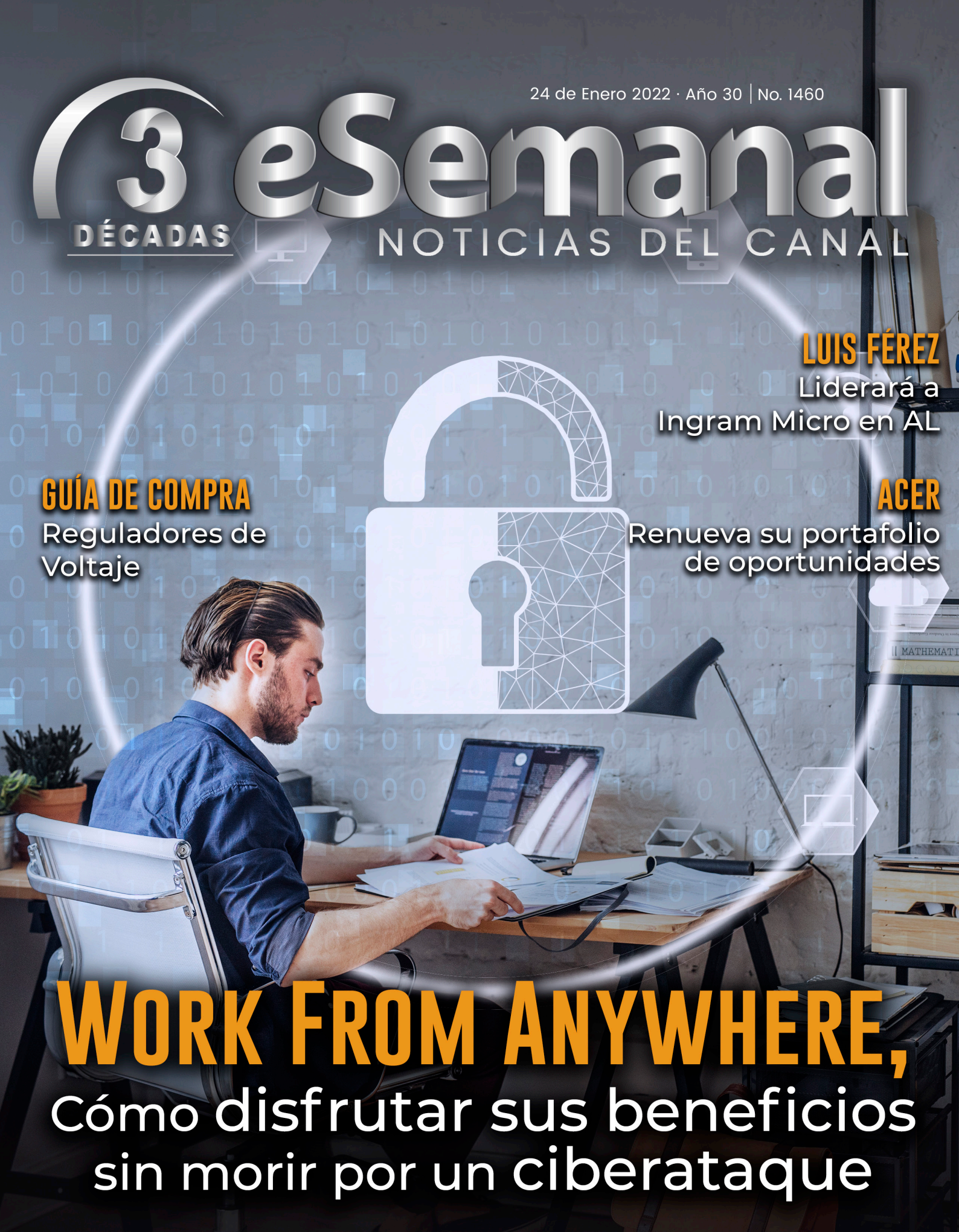
24 de Enero 2022 · Año 30 | No. 1460

3 DÉCADAS eSemanal
NOTICIAS DEL CANAL

LUIS FÉREZ
Liderará a Ingram Micro en AL

GUÍA DE COMPRA
Reguladores de Voltaje

ACER
Renueva su portafolio de oportunidades



WORK FROM ANYWHERE,

Cómo disfrutar sus beneficios sin morir por un ciberataque


¿Ya conoces nuestra
sucursal CT Guadalajara?
Ven y conoce todo nuestro inventario con precios increíbles. También puedes levantar tus pedidos en línea, o bien acércate con tu especialista CT.
¡Contamos con una excelente atención a clientes!
CT, siempre contigo.
www.ctonline.mx

Work from Anywhere una realidad que el canal debe atender

Álvaro Barriga

Las empresas cada vez más están adoptado el modelo de "trabajo desde cualquier lugar", de hecho, ya era tendencia desde antes de la pandemia, por ello están implementando nuevas medidas de ciberseguridad ante el incremento de ataques no sólo a empresas, sino directamente a usuarios; afortunadamente en México existen profesionales de desarrolladores y mayoristas especializados que cuentan estrategias para que el canal provea soluciones para este mercado.

Expertos indican que el Work from Anywhere será una de las principales modalidades laborales en este año, por lo que los hackers comenzarán a tener como objetivo los hogares y las redes personales de los altos ejecutivos, incluso oficiales de gobierno, ya que esas redes son más fáciles de comprometer que los entornos empresariales tradicionales. Ante ello resulta indispensable que las organizaciones cuenten con sistemas de seguridad robustos para defender la integridad de sus equipos ante los posibles ataques de ciberdelincuentes, cuyos métodos se harán cada vez más sofisticados.

Es necesario destacar la importancia del canal de distribución para proveer soluciones especializadas de ciberseguirdad porque es un hecho que un antivirus no es suficiente para garantizar la seguridad de la información en equipos móviles de directivos o empleados que manejan datos sensibles de las organizaciones; por ello, el canal debe tener el conocimiento del mercado, certificaciones y un portafolio de soluciones especializado, para brindar tranquilidad a sus clientes.

En esta edición, el equipo editorial de **eSemanal** entrevistó a especialistas de G Data, HP y Huawei, quienes hablaron de las principales tendencias y posibilidades de negocio para el canal en México.

Luis Férez, Vicepresidente Senior y Presidente de Latinoamérica en Ingram Micro, se dijo motivado y agradecido con el corporativo por su recién nombramiento, aseguró que 2022 será un año bueno para el negocio en la región, no con las mismas tasas de crecimiento de años anteriores a 2019, pero sí mayor a 2021.

Sin duda, el crecimiento que ha tenido Luis en Ingram Micro ha sido mérito de su capacidad de adaptarse a los cambios, a su impulso por brindar valor al mercado con soluciones especializadas y al gran equipo de trabajo que lo acompaña.

En conferencia de prensa, el directivo dejó en claro que cada país seguirá sus estrategias particulares de trabajo con canales, pero capitalizarán la infraestructura regional y corporativa.

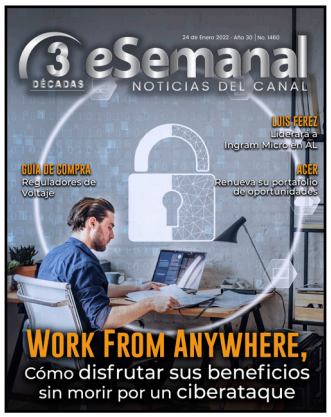
Explicó que perciben oportunidades de negocio en relacionamiento con los socios de negocio y en transaccionalidad.

¡Mucho éxito!

eSemanal noticias del canal, no recomienda equipos ni marcas, tampoco resuelve dudas técnicas individuales por teléfono. Si tiene algo que comunicarnos, diríjase a nuestras oficinas generales o use alguno de los medios escritos o electrónicos. eSemanal noticias del canal, es una publicación semanal de Contenidos Editoriales KHE, S.A. de C.V., con domicilio en Pitágoras 504-307, Col. Narvarte, C.P. 03020, México D.F. Número de certificado de reserva: 04-2013- 100817455000-102, Certificados de licitud y contenido de título: 16101, Editor responsable: Francisco Javier Rojas Cruz.
Los artículos firmados por los columnistas y los anuncios publicitarios no reflejan necesariamente la opinión de los editores. Los precios publicados son únicamente de carácter informativo y están sujetos a cambios sin previo aviso.

PORTADA

22 WORK FROM ANYWHERE, cómo disfrutar sus beneficios sin morir por un ciberataque



21 MI CUMPLE ESEMANAL

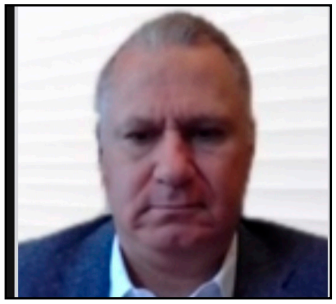
GUÍA DE COMPRA

7 Reguladores de Voltaje

GUÍA DE COMPRA

MAYORISTAS

32 Luis Férez al frente de **INGRAM MICRO** en Latinoamérica



INGRAM MICRO

FABRICANTES

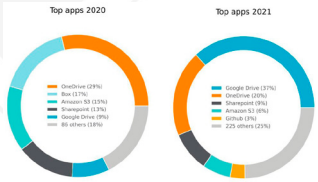
34 ACER experiencia inmersiva y sustentabilidad

45 DELL presenta nuevos equipos para impulsar la colaboración y aumentar las experiencias visuales

DELL

contactame@esemanal.mx 55 7360 5651

DESARROLLADORES



NETSKOPE

COLUMNAS

DARKTRACE

PRODUCTOS

DIRECTORIO

Editor Alvaro Barriga 55 5090-2044 alvaro.barriga@khe.mx Reporteros Anahí Nieto 55 5090-2046 anahi.nieto@esemanal.mx
Raúl Ortega 55 5090-2059 raul.ortega@esemanal.mx Redacción Web Claudia Alba 55 5090-2044 claudia.alba@khe.mx
Diseño Carmen Núñez 55 5090-2058 carmen.nunez@khe.mx Diego Hernández 55 5090-2061 diego.hernández@khe.mx
Director General Javier Rojas 55 5090-2050 javier.rojas@khe.mx Directora Administrativa Elvira Vera 55 5090-2050 elvira.vera@khe.mx
Facturación y cobranza Rebeca Puga 55 5090-2052 rebeca.puga@khe.mx Ventas de Publicidad Diego Rojas 55 5090-2053 diego.rojas@khe.mx
Suscripciones 55 5090-2049 suscripciones@khe.mx

2022

3 DÉCADAS

eSemanal

NOTICIAS DEL CANAL

Apoyando el negocio del canal

REGULADORES DE VOLTAJE

LOS REGULADORES DE VOLTAJE SE HAN CONVERTIDO EN UN ALIADO ESTRATÉGICO, PRINCIPALMENTE PARA LOS HOGARES, YA QUE AL REGULAR Y PROTEGER CONTRA LAS VARIACIONES DE VOLTAJE, AYUDA A MANTENER A SALVO LOS EQUIPOS CONECTADOS, A PROPÓSITO DE QUE ACTUALMENTE LAS PERSONAS PASAN MÁS TIEMPO EN CASA Y HACIENDO USO DE LOS MISMOS, ES POR ELLO QUE ESEMANAL PRESENTA ALGUNAS OPCIONES PARA 2022.

Texto: **Raúl Ortega**

APC Schneider Electric
LS600-LM60

Características: Protege y prolonga la vida útil de los dispositivos del hogar contra variaciones inesperadas de energía. Capacidad eléctrica de salida de 300 Watts / 600VA; Voltaje de salida nominal 120V; Voltaje nominal de entrada 120V y conexión de entrada NEMA 5-15P.

Garantía: Dos años y cambio físico en caso de falla.

APC Schneider Electric
LS1200-LM60

Características: Protege y prolonga la vida útil de los dispositivos del hogar contra variaciones inesperadas de energía. Capacidad eléctrica de salida de 600 Watts / 1200VA; Voltaje de salida nominal 120V; Voltaje nominal de entrada 120V y conexión de entrada NEMA 5-15P.

Garantía: Dos años y cambio físico en caso de falla.

CDP
R-UPR1008

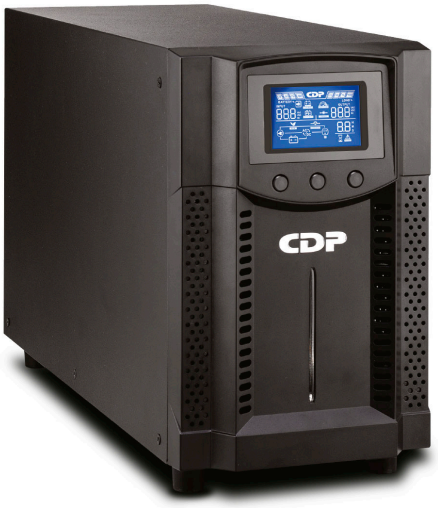
Características: Indicadores estado de UPS, breaker de protección contra sobrecarga y corto circuito, 8 contactos de salida: 2 con supresión de picos y 6 con respaldo/ regulación. Ideal para proteger: Pantallas LED/LCD, Cómputo, Audio/ Video, Telefonía, Puntos de venta, Routers, Módems, CCTV, Consolas de video y más.

Garantía: Dos años en cambio físico inmediato.

CDP
UPO11-1AX

Características: Bypass estático, paro de emergencia (EPO), onda senoidal pura a la salida, factor de potencia 1, tarjetas opcionales SNMP/Control, 4 terminales de salida NEMA 5-20R. Entrada banco de baterías externas. Ideal para centros de datos, puntos de venta, cajeros automáticos y aplicaciones industriales.

Garantía: Dos años en partes electrónicas y baterías.



ISB SOLA BASIC®

...en protección, tu única opción

XELLENCE 5000 by SOLA BASIC

REGULADOR INTELIGENTE, conjuga la robustez de un transformador de potencia tipo auto transformador de alta precisión con un microcontrolador de última generación.

Este equipo opera ininterrumpidamente en equipos que requieren **VOLTAJE DE ALTA PRECISIÓN.**

IDEAL PARA:

Equipos de análisis clínicos, dentales, ultrasonidos, rayos x , Tomógrafo
Equipos de audio y video profesionales, Estudios de Grabación

CAPACIDAD **5000** VA | **2** AÑOS de garantía

REGULADORES

MONOFÁSICO - BIFÁSICO - TRIFÁSICO

HECHO EN MÉXICO

DISPONIBLE EN:

SIGUENOS EN:

www.isbmex.com

COMPUTADORAS Y TECNOLOGÍA · cva · tecnosinergia · calcom · UNICOM · G-LOMA · CDC Group · PCH · INTCOMEX MÉXICO · EXEL · INGRAM MICRO · DC Mayorista · APOLO-TEC · Tenivisa

Complete

Energy Box 3200 / P/N ERV-10-003

Características: Regulador de voltaje con supresor de picos integrado. Ideal para línea blanca protege electrodomésticos del hogar como hornos de microondas, refrigeradores, lavadoras entre otros. Capacidad de 3200VA/1600W.

Garantía: Cinco años.

Complete

X-POWER / P/N ERV-9-001

Características: Regulador de voltaje con supresor de picos integrado. Ideal para el hogar y la oficina, brinda protección a los dispositivos audiovisuales, sistemas de entretenimiento doméstico, computadoras de escritorio. Posee 8 contactos, capacidad de 1300VA y es montable en pared.

Garantía: Cinco años.

contactame@esemanal.mx 55 7360 5651

CyberPower
CL1500VR

Características: Ideal para el hogar y la oficina, la serie CL tiene una función de regulación automática de voltaje (AVR) incorporada para ofrecer energía de CA estabilizada, especialmente adecuada para áreas con servicios públicos inestables o para uso con generadores. Los reguladores tienen tomacorrientes integrados protegidos contra sobretensiones y picos de voltaje, filtro EMI y protección contra sobrecargas para proteger el equipo conectado. El regulador de voltaje está equipado con un indicador LED para mostrar el estado de la energía.

Garantía: Dos años.

CyberPower
CL2000VR

Características: Ideal para el hogar y la oficina, la serie CL tiene una función de regulación automática de voltaje (AVR) incorporada para ofrecer energía de CA estabilizada, especialmente adecuada para áreas con servicios públicos inestables o para uso con generadores. Los reguladores tienen tomacorrientes integrados protegidos contra sobretensiones y picos de voltaje, filtro EMI y protección contra sobrecargas para proteger el equipo conectado. El regulador de voltaje está equipado con un indicador LED para mostrar el estado de la energía.

Garantía: Dos años.

DataShield
RAD-2000

Características: Ofrece potencia de 2000VA/1000W, rango de voltaje 95-150VCA, interruptor térmico breaker, hasta 8 conectores para proteger de sobrecargas o variaciones de voltaje. Ideal para proteger línea telefónica/modem, consolas de videojuegos, equipo de cómputo, audio y video.

Garantía: Dos años.

Eaton
5P de Torre (750 - 3000 VA)

Características: El UPS ofrece máxima protección y eficiencia de hasta un 99%. Ofrece un 20% más de vatios de potencia en comparación a los UPS tradicionales. La tecnología ABM, exclusiva de Eaton, aumenta la vida de las baterías en un 50%.

Garantía: Un año contra defectos de fabricación en electrónica y/o baterías.

Koblenz®

MARCA No 1 EN ENERGÍA

UPS On line

G21 TRIFÁSICO

300021 OL 3P

- **30000 VA / 27000 W**
- **El banco de baterías se vende por separado**
- **Factor de potencia .9**
- **Tecnología de DSP** que garantiza un alto rendimiento
- **Garantía del Equipo:** 3 años, 2 en batería

Capacidades disponibles: 15, 20, 30 y 40 KVA's

Ideal para:

Servidores | Equipos Médicos | Redes | Telecomunicaciones | VoIP

MAYORISTAS

Zaira Delgadillo Product Manager Koblenz zaira.delgadillo@ctin.com.mx (662) 109 0000 Ext. 189	Christian Tapia Product Manager ctapia@grupocva.com (33) 3268 1617	Mario Cervantes Product Manager Mario.Cervantes@ingrammicro.com (55) 4598 0633	Jonathan Cortés Product Manager jcortes@daisytek.com.mx (55) 5000 3518 ext. 3520	Norma Hernández Product Manager pm.marcas3@gloma.mx (871) 722 5321 ext. 210	Jazmín Martínez Product Manager jazmin.martinez@dcm.com.mx (55) 5262 5700 ext. 6018	Francisco Gómez García Product Manager fgomezgarcia@unicom.com.mx (818) 151 7500	Jorge Carranza Product Manager Jorge.carranza@pchmayoreo.mx (33) 1368 4350 ext. 4373	Juan Martínez Trejo Product Manager juan.trejo@exel.com.mx (55) 5078 4120 ext. 3159

Eaton

5S (700 - 1500 VA)

Características: El UPS brinda mayor potencia en menor espacio, protección premium en diseño de torre. La pantalla LCD de última generación ofrece una interfaz gráfica que proporciona toda la información crítica del UPS de manera local. Además, permite un ahorro en el consumo de energía de hasta el 30% gracias a la tecnología de EcoControl.

Garantía: Tres años contra defectos de fabricación en electrónica y/o baterías.

GHIA

GVR-013

Características: Ofrece potencia de 1300VA y 600W, breaker de protección contra sobrecarga y corto circuito, 3 leds indicadores, indicador de modo encendido, indicador de voltaje alto e indicador de voltaje bajo, cuenta con ocho contactos de salida, cuatro con regulación, más cuatro con supresión de picos. Ayuda a proteger: pantallas LED/LCD, routers, módems, cómputo, audio/ video, entretenimiento y más.

Garantía: Tres años.

GHIA

GVR-020

Características: Ofrece potencia de 2000VA y 800W, breaker de protección contra sobrecarga y corto circuito, 3 leds indicadores, indicador de modo encendido, indicador de voltaje alto e indicador de voltaje bajo, cuenta con ocho contactos de salida, cuatro con regulación, más cuatro con supresión de picos. Ayuda a proteger: pantallas LED/LCD, routers, módems, cómputo, audio/video, entretenimiento y más.

Garantía: Tres años.

ISB Sola Basic

CVR2500

Características: Ofrece potencia de 2500VA. Regulador automático especialmente diseñado para mantener niveles óptimos de voltaje. Para aquellos equipos que inclusive utilicen motor. Protege contra las severas variaciones de tensión de suministro eléctrico. Ideal para línea blanca como refrigeradores, microondas, centros de lavado y bombas de agua.

Garantía: Dos años.

jmgabbai@isbmex.com

ISB Sola Basic

XELENCE 5000

Características: Ofrece potencia de 5000 VA, regulador inteligente, conjuga la robustez de un transformador de potencia tipo auto transformador de alta precisión y microcontrolador de última generación. Este equipo opera ininterrumpidamente en equipos que requieren voltaje de alta precisión. Ideal para equipos de análisis clínicos, dentales y ultrasonidos.

Garantía: Dos años.

jmgabbai@isbmex.com

Koblenz
ER-2250

Características: Regulador electrónico de voltaje, nivel de protección GOLD con capacidad de 2250VA/1000W, cuenta con 8 contactos tipo NEMA 5-15R en la parte superior, sistema de desconexión por alto voltaje, póliza de seguro en equipo conectado por hasta 10000 dólares, ideal para equipos de audio y video.

Garantía: Cinco años.

moralesh@koblenz.com

Koblenz
RS-1410

Características: Regulador electrónico de voltaje con potencia de 1410VA/700W, moderno diseño con ocho contactos en la parte superior, led indicador de funcionamiento, interruptor de encendido y apagado de uso rudo, sistema de desconexión. Ideal para conectar equipo de cómputo, televisores y sistemas de audio.

Garantía: Dos años.

moralesh@koblenz.com

Steren
REG - 1050

Características: Ayuda a mantener tus aparatos a salvo de las fallas que se presentan en el suministro de energía eléctrica, protege tus dispositivos electrónicos contra sobrecargas, cortocircuitos, variaciones y picos de voltaje (40 Joules). Carga hasta 1000 W, por lo que puedes conectar pantallas, consolas de videojuegos, equipo de sonido, computadoras y más. Tiene protección de línea telefónica/ módem. Incorpora 8 salidas para clavijas americanas y/o europeas.

Garantía: Un año.

Steren
REG - 2050

Características: Protege aparatos electrónicos delicados contra variaciones y picos de voltaje, como corto circuito y sobrecarga. Tiene capacidad máxima de carga de 2000 W, incorpora 8 contactos polarizados de salida, tiene luces LED que indican el encendido del equipo y estado de regulación. Incorpora 2 conectores RJ12 en uno de sus costados para protección de línea telefónica o módem.

Garantía: Un año.

Tripp Lite
LC1200

Características: Ofrece 4 tomacorrientes NEMA 5-15R con regulación automática de voltaje para corregir caídas y sobrevoltajes graves desde 89V a 147V a una potencia nominal regulada de 120V, filtra el ruido de línea, monitorea el estado de energía con LED de diagnóstico en el panel frontal y es de grado informático.

Garantía: Limitada de dos años.

Tripp Lite
LS606M

Características: Ofrece 6 tomacorrientes NEMA 5-15R con regulación automática de voltaje, para corregir caídas y sobrevoltajes graves desde 85V a 147V, a una potencia nominal regulada de 120V, filtra el ruido de línea, monitorea el estado de energía con LED de diagnóstico en el panel frontal y es de grado informático.

Garantía: Limitada de dos años.

Vorago
AVR-100

Características: Regulador con supresor de 8 contactos, 1000 VA. Protección de altibajos de corriente que al mismo tiempo regulan el voltaje y lo mantienen uniforme hasta para 4 equipos.

Garantía: Un año.

Vorago
AVR-200

Características: Protección de los picos de corriente con los 8 contactos del regulador de voltaje, que al mismo tiempo regulan el voltaje y lo mantienen uniforme hasta para 4 equipos.

Garantía: Un año.

FELICITA

Lunes 24

EDGAR DÍAZ ZAMUDIO, GERENTE GENERAL DIVISIÓN HARDWARE EN DE *ATIO*

EDUARDO BELTRÁN SÁNCHEZ, ADMINISTRADOR EN *SIBC*

GUILLERMO PADILLA MORALES, COORDINADOR DE MERCADOTECNIA EN *FIBRAS ÓPTICAS DE MÉXICO*

Martes 25

ELVIRA HERNÁNDEZ RODRÍGUEZ, SUBDIRECTORA DE VENTAS EN *NACEB*

ISMAEL HERRERA MORALES, DIRECTOR DE VENTAS Y MERCADOTECNIA EN *COMUNÍCALO DE MÉXICO*

Miércoles 26

RICARDO GARCÍA, DIRECTOR DE OPERACIONES EN *INGRAM MICRO*

SANDRA GÁLVEZ SÁNCHEZ, MARKETING MANAGER LATAM EN *KODAK ALARIS*

Jueves 27

ERICK VELASCO HERNÁNDEZ, CHANNEL & SMB SALES MANAGER MEXICO EN *TP-LINK TECHNOLOGIES*

SILIMEX POR SU *53 ANIVERSARIO*

Viernes 28

ANGÉLICA FIGUEROA, MARKETING EN *ISSABEL*

HÉCTOR FUENTES OLMOS, GERENTE DE VENTAS EN *MLM MULTISERVICIOS*

KEES VAN RONGEN, DIRECTOR DE *ACER MÉXICO*

LUIS GARCÍA MARTÍNEZ, DIRECTOR GENERAL DE *ALTO IMPACTO*

MANUEL CANCINO ROMERO, VENTAS IP PBX EN *PANASONIC DE MÉXICO*

SARA ÁNGEL ACOSTA, PRODUCT MANAGER VORAGO EN *INGRAM MICRO*

VERSION POR SU *30 ANIVERSARIO*

Sábado 29

FRANCISCO ADAME, SUB DIRECTOR DE CANALES MAYOREO EN *HISENSE MÉXICO*

MARIANA CEJUDO CONTRERAS, GERENTE DE MARKETING Y GENERACIÓN DE *DEMANDA EN ERP SOLUCIONES*

Domingo 30

HÉCTOR IBARGÜEN JR., EJECUTIVO DE VENTAS ZONA OCCIDENTE EN *NACEB*

CORSAIR POR SU *28 ANIVERSARIO*

ERO 2022

3 DÉCADAS eSemanal NOTICIAS DEL CANAL

WORK FROMANYWHERE, CÓMO DISFRUTAR SUS BENEFICIOS SIN MORIR POR UN CIBERATAQUE

Texto: Anahi **Nieto**

- EN 2020, MÉXICO FUE EL PAÍS MÁS ATACADO DE LATINOAMÉRICA
- 7 DE CADA 10 AMENAZAS TUVIERON COMO OBJETIVO A TRABAJADORES REMOTOS
- LÍDERES EMPRESARIALES PLANEAN INCREMENTAR SU INVERSIÓN EN CIBERSEGURIDAD

Aunque ya era una tendencia, desde hace dos años la pandemia provocó que el concepto "Work From Anywhere" (WFA) se consolidara y se volviera una realidad para millones de personas en el mundo, gracias a las múltiples ventajas que este esquema de trabajo implica, la principal, resguardar el distanciamiento social y la salud.

Otros beneficios de este modelo de trabajo son que las personas pueden administrar mejor su tiempo, estableciendo un equilibrio entre sus actividades laborales y su vida privada, elegir el espacio que prefieran y donde se sientan más cómodos, y ser así más productivos.

Giovanni Loarte, líder de Soporte Técnico en G Data, explicó que el WFA hizo posible la movilidad en el trabajo para garantizar la continuidad del negocio ante la pandemia, aspecto que hizo crecer su adopción de forma exponencial.

A pesar de las diferentes ventajas que proporciona este esquema, la seguridad cibernética ha sido el desafío primordial para ponerlo en práctica, lo cual ha dejado expuestas a miles de compañías y las ha obligado a configurar una nueva estrategia de ciberseguridad.

Las empresas han adoptado este modelo de trabajo y esto conllevó a implementar nuevas medidas de ciberseguridad, al principio de la pandemia fue más complejo tener un estrategia en este ámbito para este esquema de trabajo; sin embargo, hoy en día existen empresas como G Data que pueden brindar un alcance de protección muy bueno para el trabajo desde cualquier lugar.

GIOVANNI **LOARTE**

"LO PELIGROSO DE ESTE MODELO ES QUE DÍA A DÍA GENERA MÁS BRECHAS DE CIBERSEGURIDAD, IMPULSADAS POR LA MISMA CONSUMERIZACIÓN, LO QUE EXPONE A LOS USUARIOS CON FALTA DE CULTURA INFORMÁTICA, ORDENADORES, TELÉFONOS INTELIGENTES, ETCÉTERA; POR ELLO, ES IMPORTANTE QUE LAS ÁREAS ENCARGADAS DE CIBERSEGURIDAD EN LA EMPRESAS BUSQUEN ALTERNATIVAS DE SOLUCIONES PARA OFRECER UN ECOSISTEMA DE PROTECCIÓN COMPLETO, YA QUE AL TENER MÁS HERRAMIENTAS, SE REDUCEN SIGNIFICATIVAMENTE LAS BRECHAS": GIOVANNI LOARTE.

Rendimiento y productividad.

HP ProBook 440 G8

Conoce más

Procesadores Intel® Core™

SmartBid

Las amenazas principales

El directivo de G Data dio a conocer las cuatro amenazas principales que el laboratorio ha detectado existen para el teletrabajo:

1.- Cryptojacking: la minería de criptomonedas maliciosa ha tenido un aumento en esta pandemia. Utiliza los recursos de la máquina para extraer diversas formas de monedas digitales conocidas como criptomonedas. Es una amenaza floreciente que puede apoderarse de navegadores web, así como comprometer todo tipo de dispositivos, desde ordenadores de escritorio y portátiles hasta teléfonos inteligentes, e incluso servidores de red.

2.- Ransomware: una de las amenazas más persistentes y que continúa su crecimiento debido al gran retorno económico que derrama para la ciberdelicuencia. Lo más peligroso es que ahora se identifica un Ransomware más sofisticado que se expande con gran rapidez a sistemas operativos menos comunes como MacOS o Linux.

3.- Campañas de phishing (estafas por medio de correo electrónico): si bien este ataque es de los más comunes, ahora los ciberdelicuentes hacen uso de Inteligencia Artifical (IA) que puede simplificar búsquedas de objetivos y dirigir ataques más personalizados (Spear phishing), con la intención de poder detectar de forma sencilla; por ejemplo, si algún usuario tiene tarjeta de crédito y personalizarle un phishing.

4.- Ataques por fuerza bruta a protocolo RDP: debido a la alta demanda y premura de las empresas para continuar en un trabajo remoto, los servidores se configuraron de forma incorrecta, estas vulnerabilidades permiten a los cibercriminales ejecutar ataques de fuerza bruta para adivinar las credenciales y poder ganar acceso al servidor.

CON BASE EN EL ANÁLISIS DE AMENAZAS PARA 2022 DE G DATA, SE CONSIDERA QUE CONTINUARÁN EXISTIENDO:

Cryptojacking
Ransomware
Phishing
Ataques a microservicios en la nube
Ataques a dispositivos móviles

¿Cómo protegerse?

Con el fin de evitar ser víctima de un ciberataque, el directivo de G Data recomendó a las empresas implementar una estrategia de ciberseguridad en la que principalmente puedan hacer un análisis de riegos de sus activos, con la intención de saber cuáles de estos son los más sensibles y donde mayor impacto pueda tener para el negocio en caso de que se materialice un evento de ciberseguridad.

Con base en el análisis, se deben de establecer las acciones a tomar para controlar o mitigar los riesgos, donde se recomienda incluir distintas capas de seguridad, comenzando por lo más básico, por ejemplo: política de contraseñas seguras, control de acceso a usuarios, software de antivirus, firewall perimetral, WAF, IPS, HoneyPot, entre otros. “Las medidas pueden ser muchas; sin embargo, es necesario tener el conocimiento previo de nuestros riesgos para recomendar las mejores prácticas y tratamientos de ciberseguridad”.

“Con relación a los usuarios, es importante mantenerlos actualizados con cursos de concientización que les enseñen a identificar un correo malicioso o una página fraudulenta, ya que ellos normalmente son una de la capas más vulnerables en la cadena de ciberseguridad; desde luego sus ordenadores también deben contar con ciertos controles como: evitar que trabajen con privilegios de administrador, tener un antimalware, como G Data, por ejemplo, que pueda control las conductas inapropiadas bloqueando accesos a sitios web prohibidos, aplicaciones de ocio, entre otros”, enfatizó Loarte.

Por su parte, Martín Portillo, Director de Ciberseguridad para Huawei México, explicó que recomendaciones básicas obligatorias para un teletrabajo seguro tienen que ver con procesos operativos y herramientas actualizadas. Las cuales se pueden resumir en:

-Mantener el uso de licencias de software actualizadas

-Uso de antivirus recomendado por su empresa o su proveedor de licencias

-Preferentemente usar VPNs (Red Privada Virtual) para conectarse con clientes o a la empresa

-Cambio frecuente de passwords (combinación de números, letras y caracteres especiales)

-Capacitación básica sobre esquemas típicos de ciberataques y protección a los mismos

“De acuerdo con el IFT, en 2020 México fue el país más atacado en Latinoamérica, al recibir el 22.57% de alrededor de 1.3 millones de ataques de ransomware (secuestro de datos para pedir rescate), a 297 mil empresas. Se ha encontrado también que las empresas han tenido que pagar 14 millones de dólares por ataques de ransomware”, explicó Martín Portillo.

MARTÍN **PORTILLO**

contactame@esemanal.mx 55 7360 5651

3 DÉCADAS

eSemanal

NOTICIAS DEL CANAL

CONOCE NUESTROS SERVICIOS DIGITALES

- Estratégias comerciales
- Soluciones de comunicación
- Oportunidades de negocio

www.esemanal.mx ventas@esemanal.mx

“El 2022 trae consigo oportunidades y desafíos muy relevantes en temas de ciberseguridad, la generalización cada vez más evidente del uso de tecnología (TICs) para nuestro día a día, que en otras palabras implica la digitalización de nuestra vida, además de los beneficios obvios que esto trae, también nos acompañará con riesgos de vulnerabilidad de nuestra identidad (incluyendo datos biométricos), transacciones bancarias (información financiera en general) lo cual implicaría sin temor a exagerar, riesgos para la vida misma”, añadió Portillo.

Todo lo anterior, de acuerdo con el directivo, obliga a poner especial atención en las herramientas y procedimientos de trabajo que minimizarán o al menos disminuirán los potenciales riesgos del teletrabajo o WFA.

“Cuando hablamos de tendencias y para resumir, veremos básicamente tres fenómenos: incremento de la oferta y demanda de capacitación en procesos y esquemas de ciberseguridad, aparición de compañías especializadas en ofrecer marcos de apoyo y protección de la información y naturalmente el reforzamiento de las herramientas tanto de hardware como de software orientadas a un ciberespacio seguro”, destacó Portillo.

Otras recomendaciones para mitigar los riesgos dadas a conocer por Ricardo Castillejo, Gerente de Producto de Notebooks Empresariales en HP México, son: aplicar los principios de confianza cero —acceso de mínimo privilegio, aislamiento, control de acceso obligatorio y una gestión de identidades sólida— las organizaciones pueden reducir drásticamente la superficie de ataque y asegurar el futuro del trabajo.

En tanto, los usuarios que busquen protegerse ante un posible ciberataque deben seguir las recomendaciones básicas de seguridad de los equipos gestionados, las cuales incluyen: no compartir su información personal a través de redes públicas y no confiar en ligas o correos sospechosos con el objetivo de evitar el robo de información sensible.

contactame@esemanal.mx 55 7360 5651

Hardware y Software, juntos por la seguridad

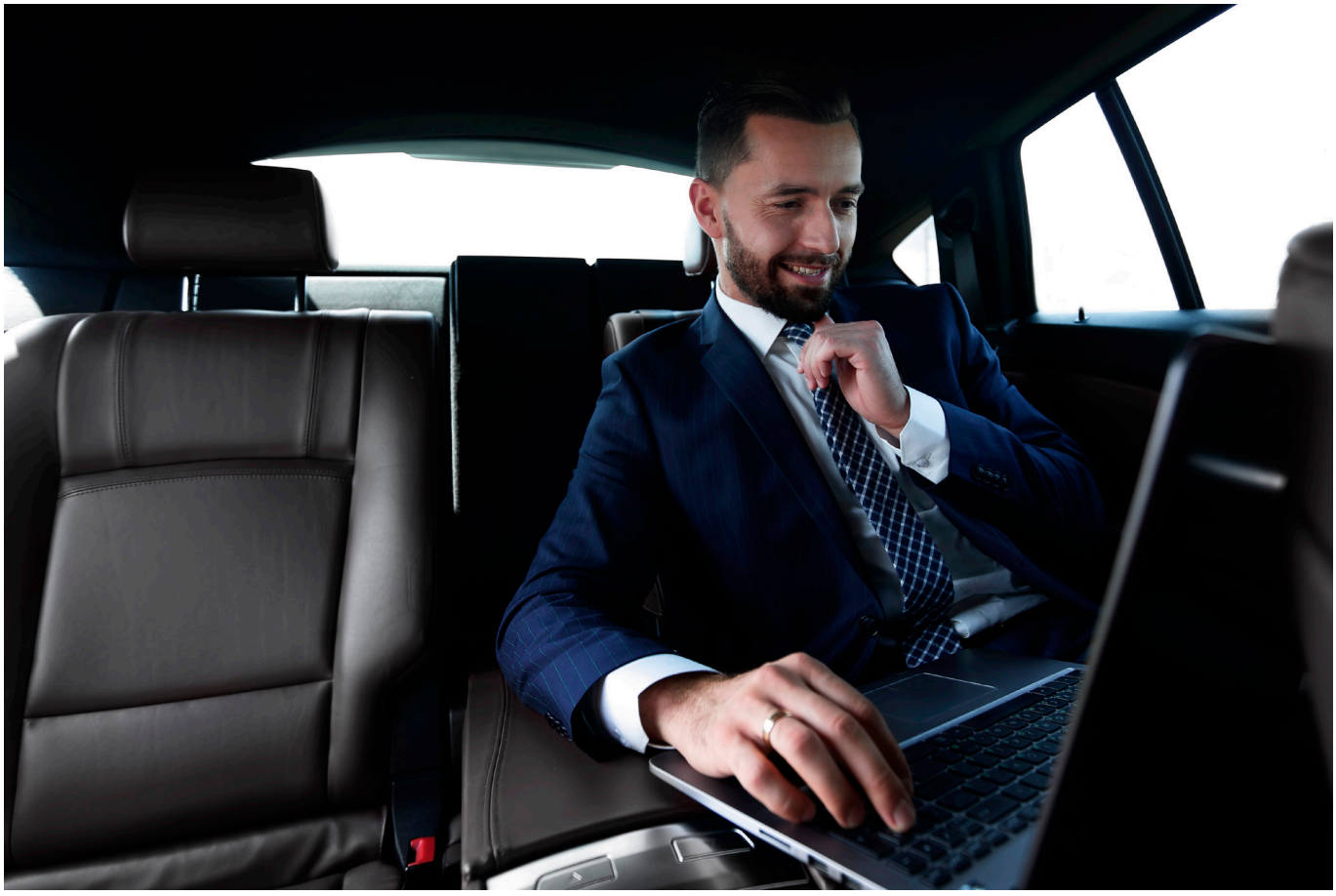
El directivo de Huawei también explicó que las nuevas plataformas tecnológicas que se empiezan a desplegar nacen ya con estructuras tanto de hardware como de software que permiten optimizar los procesos de prevención, detección y recuperación de potenciales ataques. "En el rubro de teletrabajo, siempre será recomendable contar con equipos robustos y actualizados capaces de aprovechar las optimizaciones ofrecidas por las nuevas generaciones de tecnología que tendremos a nuestro alcance".

En el mismo sentido, Castillejo comentó que HP Wolf Security puede ayudar a las organizaciones a defenderse en contra de la abundancia de nuevos ataques y riesgos que les harán frente en 2022, ya que combina software reforzado por hardware y características de seguridad con servicios de seguridad endpoint, proporcionando privacidad e inteligencia de amenazas, y reuniendo datos en el dispositivo endpoint para ayudar a proteger a la empresa en general.

RICARDO **CASTILLEJO**

"El cambio al trabajo híbrido seguirá creando problemas para la seguridad organizativa ya que cada uno de los empleados continuará siendo un objetivo potencial para los atacantes, lo cual podrá crear una importante brecha de seguridad debido a la gran cantidad de dispositivos inseguros y no gestionados, los cuales son más difícil de defender".

"Frente a un panorama en el que el trabajo desde cualquier lugar continuará siendo una de las principales modalidades laborales en 2022, los actores de las amenazas podrían empezar a



tener como objetivo los hogares y las redes personales de los altos ejecutivos, incluso oficiales de gobierno, ya que estas redes son más fáciles de comprometer que los entornos empresariales tradicionales. Ante estas circunstancias, resulta indispensable que las empresas cuenten con sistemas de seguridad robustos para defender la integridad de sus equipos ante los posibles ataques de cibercriminales cuyos métodos se harán cada vez más sofisticados", advirtió Castillejo.

El directivo también mencionó que las cadenas de suministro probablemente continuarán ofreciendo nuevas oportunidades para los actores de las amenazas en 2022. Además, las organizaciones también deben estar conscientes de la amenaza que representan las vulnerabilidades en un software de código abierto, ya que a lo largo de este año se verá un aumento en los paquetes de software de código abierto que se incorporan a las cadenas de suministro enfocadas en este rubro. Esto podría llevar a que más compañías estén comprometidas, independientemente de si tienen un perímetro seguro o una buena posición en general.

No es un dato nuevo que la industria cibercriminal se actualiza de forma constante y crea amenazas más sofisticadas; no obstante, los fabricantes también trabajan continuamente en proporcional a los usuarios soluciones más confiables que logren mitiguen los ataques y minimicen los riesgos.

De acuerdo con un estudio reciente de Forrester Consulting comisionado por Tenable, el 96% de las organizaciones experimentó al menos un ciberataque en el negocio, alarmante cifra que elevó las alertas de los líderes mexicanos, ya que un ciberataque a los activos críticos puede ser devastador para el negocio.

Además, 7 de cada 10 de los ciberataques a organizaciones mexicanas tuvieron como objetivo a trabajadores remotos; el 59% de los líderes de seguridad mexicanos afirmaron no tener visibilidad sobre las prácticas de seguridad en el hogar de los empleados remotos.

En este contexto, los líderes empresariales y de seguridad están mirando hacia adelante y planean aumentar las inversiones en seguridad de red en un 88%, la gestión de vulnerabilidades en un 79%, y seguridad en la nube con 75% en los próximos 1-2 años, según el mismo estudio.

contactame@esemanal.mx 55 7360 5651

3 DÉCADAS

eSemanal

NOTICIAS DEL CANAL

SÍGUENOS EN TWITTER

@eSemanal

LUIS FÉREZ AL FRENTE DE INGRAM MICRO EN LATINOAMÉRICA

Autor: Anahi **Nieto**

• CONTINUARÁN ESTRATEGIA DE CRECIMIENTO EN LA REGIÓN Y APOYOS AL CANAL, CON PROGRAMAS Y FINANCIAMIENTO.

Ingram Micro anunció a Luis Férez como el nuevo vicepresidente senior y presidente para América Latina, quien se dijo motivado por la oportunidad y agradecido por el profesionalismo, compromiso y resultados de su equipo, con el cual continuará trabajando de la mano para expandir la estrategia de la región al resto del mundo.

El directivo expuso que el 2021 fue el mejor año en la historia de la región para la compañía debido al crecimiento del 50% y reafirmó su compromiso para que sigan siendo un mayorista exitoso.

"Estamos creciendo, tenemos la visión de ir hacia adelante, el futuro se ve prometedor; estamos en la industria adecuada, en la cual hemos ayudado a los negocios a salir adelante. Continuaremos creciendo y conquistando los retos del futuro, seguiremos trabajando de cerca con el canal y pondremos al cliente en el centro de la estrategia", enfatizó Férez.

Pilares estratégicos

Los pilares estratégicos para Ingram Micro serán Cloud, división que creció más del 50% en la región, y buscan crear una visión unificada en LATAM; lanzarán el Marketplace en Miami, y continuarán complementando el catálogo y ampliando la oferta con más fabricantes. En Colombia, 300 canales transaccionales forman parte del marketplace.

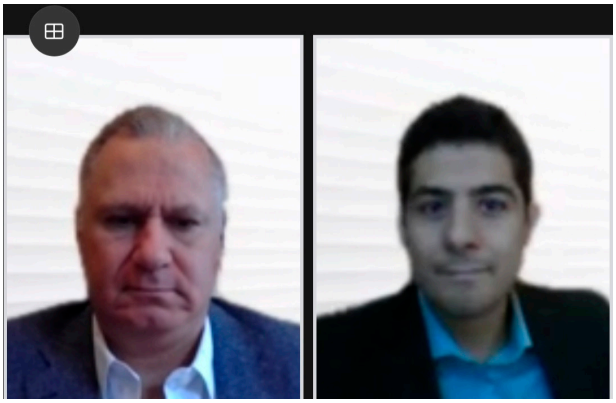
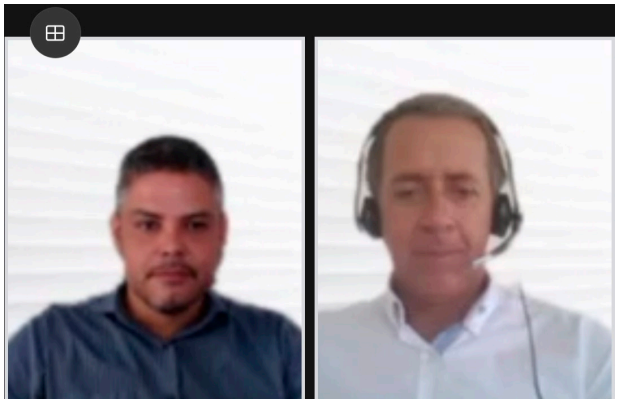
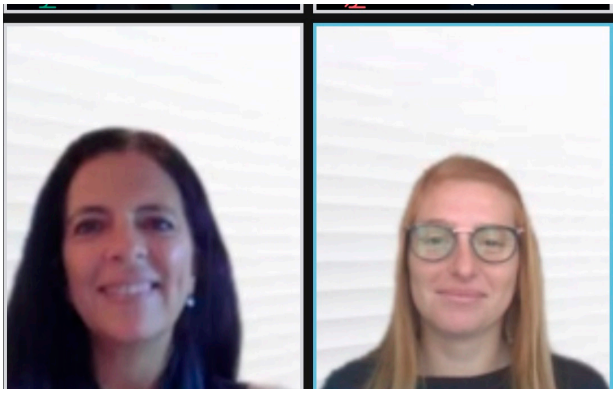
Technologies Solutions es otra de las divisiones que crece a pasos agigantados y en donde encuentran oportunidades para relacionarse y transformase de ser canales transaccionales a canales que aporten mayor valor.

"La compañía trabaja en su digitalización, pero va más allá de eso con plataformas que nos ayuden a satisfacer las necesidades que hoy en día tienen los usuarios, que apoyen en el manejo de facturación recurrente, y los servicios X As a Service", agregó Férez.

Business Intelligence es una estrategia interna que forma parte de sus pilares, y es utilizada para tener un mejor manejo de la información que se recauda y poder lograr una mejor colaboración con el canal en donde se encuentren mejores oportunidades de productividad y eficiencia para mejorar los nuevos negocios.

Advanced Solutions es otra de las divisiones donde se espera una mayor inversión por parte del mercado de data centers e identifican oportunidades relevantes en infraestructura para los usuarios. De igual forma, la videocolaboración, la ciberseguridad, y el Internet de las Cosas traerán oportunidades impor-

contactame@esemanal.mx 55 7360 5651


tantes, éste último con soluciones empaquetadas en Estados Unidos que se buscan expandir a México.

Trabajo cercano con el canal

Según se dio a conocer durante la rueda de prensa virtual, la estrategia con el canal continuará fortaleciéndose, principalmente con la estrategia One LATAM para comunicar las acciones con el cliente; además permanecerán las actividades de desarrollo para el canal, a través del Programa Commit, donde se les preparará para vender soluciones.

"Por medio del Programa Commit, ayudamos a desarrollar a los partners con advanced solutions, se recluta a los canales que tienen las características para ser éxitos en la venta de soluciones y los entrenamos para que mejoren sus habilidades y puedan vender soluciones. Ha sido un programa muy exitoso", detalló Daniela Rosa, vicepresidente OCCE Latam Export & Advanced Solutions LATAM.

Aunque aún se pronostican oportunidades para la venta de cómputo y colaboración, el 2022 se presenta como un año bueno para la implementación de soluciones, a pesar del nivel maduro que la región tiene en el negocio de soluciones, se espera que continúe el crecimiento.

Algunas acciones exitosas que han tenido de forma particular los países de Latinoamérica serán replicadas en el resto de los países; por ejemplo, en Colombia la venta de soluciones abarca el 55%, mientras que en México sólo es del 20%, y por lo tanto consideran que existe la oportunidad de seguir creciendo el negocio.

En contraparte, Colombia busca retomar la división de Servicios Profesionales que México implementó. Mientras tanto, en Chile el consumo electrónico es un negocio fuerte, como en Brasil lo es Cloud.

Respecto a los retos que Luis Férez identifica para el canal, el financiamiento resulta ser la limitación más grande en la región para que el negocio de "todo como servicio" explote: "estamos trabajando para traer opciones financieras que se adecúen a los diferentes segmentos de negocio. Trabajamos en robustecer nuestro catálogo de relaciones comerciales".

El otro reto consiste en que hoy en día la venta de tecnología resulta más compleja que antes, ya que se requiere un mayor conocimiento técnico y experiencia para vender una solución al usuario final; es por ello que las alianzas serán un tema fuerte e importante, tanto con los mayoristas y con otros canales.

3 DÉCADAS eSemanal NOTICIAS DEL CANAL

ACER, EXPERIENCIA INMERSIVA Y SUSTENTABILIDAD

Texto: Anahi Nieto

Recientemente, se llevó a cabo el "Acer Reveal Virtual Immersive Experience 2022", en donde el fabricante dio a conocer sus principales anuncios para el año y brindó una experiencia inmersiva con el uso de sus soluciones.

Gregg Prendergast, president, Acer Pan America, dio la bienvenida al evento que durante tres días mostró su propuesta para atender a un mercado que durante la pandemia cambió su forma de consumir tecnología, en especial para las distintas necesidades de las personas.

En tanto, Rich Black, vice president for Pan America Marketing en Acer, explicó que las innovaciones de la compañía en notebooks y accesorios están encaminadas hacia la sustentabilidad, bajo el compromiso de Earthion, al utilizar materiales reciclados y resistentes, así como tecnología de vanguardia.

GREGG PRENDERGAST

contactame@esemanal.mx 55 7360 5651

La iniciativa del fabricante busca contribuir a la formación de un mundo mejor en el que no se quede huella ni impacto ambiental.

Objetivos de la iniciativa Earthion

-Para el 2025, la compañía planea alcanzar un 60% de energía renovable, y el 100% de energía renovable (RE100) para el 2035.

-Para 2025, esperan alcanzar un 30% de contenido de plástico PCR en los productos principales.

-De igual forma, para el año 2025, se planea que el 80% de los proveedores fundamentales estén comprometidos con RE100.

-Comparado con el año 2009 como referencia, para el 2050 Acer tiene el objetivo de reducir el carbono en un 80%.

-Se espera que los productos del fabricante consuman un 45% menos de energía para el 2025, en comparación con el año 2016 como referencia.

-Además, perseguirán la meta de que el 100% del embalaje de la computadora portátil esté fabricado con materiales sustentables.

RICH **BLACK**

3 DÉCADAS

eSemanal

NOTICIAS DEL CANAL

SÍGUENOS CON UN

/Revista eSemanal

www.esemanal.mx

3 DÉCADAS eSemanal NOTICIAS DEL CANAL

LA PROTECCIÓN CONTRA MALWARE EN APLICACIONES EN LA NUBE ABRE OPORTUNIDADES

Autor: Anahi **Nieto**

•MÁS DE DOS TERCIOS DE LAS DESCARGAS DE MALWARE EN 2021 PROVENÍAN DE APLICACIONES EN LA NUBE
•GOOGLE DRIVE ARREBATA A MICROSOFT ONEDRIVE EL PRIMER PUESTO EN DESCARGAS DE MALWARE MIENTRAS QUE LOS DOCUMENTOS DE OFFICE MALICIOSOS CASI SE DUPLICAN

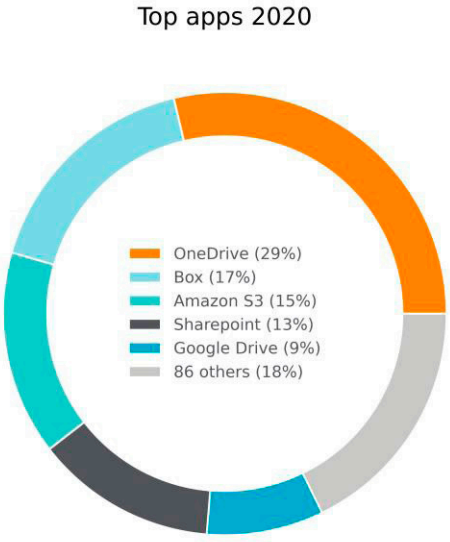
El fabricante especializado en la seguridad desde la nube, presentó su más reciente Cloud and Threat Report de enero 2022, donde pone especial atención al crecimiento continuo del malware, así como otros archivos maliciosos entregados por aplicaciones en la nube, lo que si bien, es un problema que se agrava, también son oportunidades capitalizables para entregar soluciones en ciberseguridad que estén a la altura de lo que el mercado demanda.

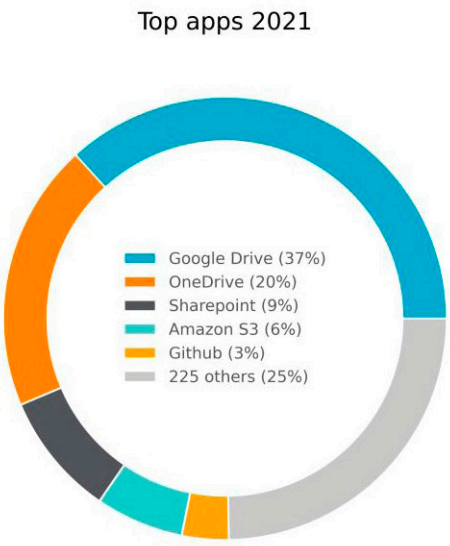
Redacción eSemanal

La investigación busca poner foco a las principales amenazas que existen en la nube y los riesgos de los datos en 2021, además, también definió los cambios en el panorama del malware durante todo el 2021, donde los ciberdelincuentes logran un mayor éxito en la entrega de cargas útiles de malware a sus víctimas, lo que resulta alarmante, al tiempo que da cuenta de la creciente oportunidad de negocio que existe para los canales especializados en ciberseguridad.

Quizás, una de las revelaciones que permiten dimensionar el tamaño de la problemática del malware, Netskope la identificó a partir de que, más de dos tercios de las descargas de malware en 2021 provinieron de aplicaciones en la nube, identificando a Google Drive como la aplicación con más descargas de malware durante el pasado año, desplazando a Microsoft OneDrive del primer puesto.

"LA CRECIENTE POPULARIDAD DE LAS APLICACIONES EN LA NUBE HA DADO LUGAR A TRES TIPOS DE ABUSO DESCRITOS EN ESTE INFORME: ATACANTES QUE INTENTAN OBTENER ACCESO A LAS APLICACIONES EN LA NUBE DE LAS VÍCTIMAS, ATACANTES QUE SE APROVECHAN DE LAS APLICACIONES EN LA NUBE PARA DISTRIBUIR MALWARE Y PERSONAL MALINTENCIONADO QUE UTILIZAN APLICACIONES EN LA NUBE PARA LA EXFILTRACIÓN DE DATOS, POR LO QUE, EL INFORME SIRVE COMO RECORDATORIO DE QUE LAS MISMAS APLICACIONES QUE UTILIZAMOS CON FINES LEGÍTIMOS SERÁN ATACADAS





Y UTILIZADAS DE FORMA ABUSIVA. PROTEGER LAS APLICACIONES EN LA NUBE PUEDE AYUDAR A EVITAR QUE LOS ATACANTES SE INFILTREN EN ELLAS, MIENTRAS QUE EL ANÁLISIS DE AMENAZAS ENTRANTES Y DATOS SALIENTES PUEDE AYUDAR A BLOQUEAR LAS DESCARGAS DE MALWARE Y LA EXFILTRACIÓN DE DATOS": RAY CANZANESE, DIRECTOR DE INVESTIGACIÓN DE AMENAZAS, NETSKOPE THREAT LABS.

Es importante señalar que, Netskope Cloud and Threat Spotlight, es un estudio realizado por investigadores de malware y amenazas en la nube, entregando resultados sobre tendencias, entre los que resaltan el aumento de documentos maliciosos de Office, pasando del 19% al 37% de todas las descargas de malware, lo que apunta a un aumento de riesgos de seguridad de las aplicaciones en la nube. Otro hallazgo está en que más de la mitad de todas las instancias de aplicaciones en la nube gestionadas, son objeto de ataques de credenciales.

HALLAZGOS CLAVE DEL NETSKOPE CLOUD AND THREAT SPOTLIGHT DE 2021:

- **El malware entregado en la nube ahora es más frecuente que el malware entregado vía web:** En 2021, las descargas de malware procedentes de aplicaciones en la nube aumentaron al 66% de todas las descargas de malware, en comparación con los sitios web tradicionales y frente al 46% de principios de 2020.
- **Google Drive emerge como la principal aplicación para la mayoría de las descargas de malware:** La investigación encontró que Google Drive ahora representa la mayoría de las descargas de malware en 2021, ocupando ahora el primer lugar y desplazando a Microsoft OneDrive.
- **El malware entregado en la nube a través de Microsoft Office casi se duplicó entre 2020 y 2021:** Los documentos maliciosos de Microsoft Office alcanzaron el 37% de todas las descargas de malware a finales de 2021 en comparación con el 19% a principios de 2020. Esto se debe a que los atacantes continúan usando documentos de Office infectados para conseguir un punto de acceso inicial en los sistemas objetivos de ataques. Ya que, tras la campaña "Emotet" en el segundo trimestre de 2020, se inició un incremento de documentos maliciosos de Microsoft Office y que se ha sostenido a lo largo de los últimos seis trimestres, sin signos de desaceleración.
- **Más de la mitad de las instancias gestionadas de aplicaciones en la nube son el objetivo de ataques de credenciales:** Los ciberdelincuentes prueban constantemente contraseñas comunes y credenciales filtradas de otros servicios para obtener acceso a información confidencial almacenada en aplicaciones en la nube. Si bien el nivel general de ataques se mantuvo constante, las fuentes de los ataques cambiaron significativamente, siendo el 98% de los ataques provenientes de nuevas direcciones IP.
- **La exfiltración de datos corporativos va en aumento:** Uno de cada siete empleados se lleva los datos cuando deja la empresa, utilizando instancias de aplicaciones personales. Entre 2020 y 2021, un promedio del 29% de los empleados que abandonaron su trabajo, descargaron más archivos de las instancias de aplicaciones corporativas administradas y el 15% de los usuarios cargó más archivos en las instancias de aplicaciones personales en sus últimos 30 días de trabajo.

EL FUTURO DE LA CIBERSEGURIDAD: MÁS ATAQUES A CADENAS DE SUMINISTRO DE TI'S PARA 2022

*Justin Fier.

En el 2020, el sector de los servicios financieros fue el que experimentó el mayor volumen de ciberataques. Durante años, los atacantes se han dirigido a estas organizaciones porque son objetivos previsiblemente lucrativos.

Pero en el 2021, el sector de los servicios financieros dejó de ser el más atacado. En su lugar, el sector de las tecnologías de la información y las comunicaciones, incluidos los proveedores de telecomunicaciones, los desarrolladores de software y los proveedores de servicios de seguridad gestionados, entre otros, fueron los que más sufrieron intentos de ciberataques.

Este cambio en el objetivo principal de los hackers no es una sorpresa para los expertos de la industria, dados los numerosos ataques de alto perfil a la cadena de suministro de software ocurridos en el 2021, incluyendo los de SolarWinds, Kaseya y GitLab. Los cibercriminales ven cada vez más la infraestructura, las plataformas y los proveedores de software y desarrolladores como vectores de entrada a gobiernos, empresas e infraestructuras críticas.

Los analistas de Darktrace observaron que su inteligencia artificial (IA) interrumpió de forma autónoma alrededor de 150.000 amenazas cada semana contra este sector en el 2021. Estas conclusiones de investigación se elaboran a partir de los datos de Darktrace generados por el "análisis de indicadores tempranos", que examina los rastros (también llamados "migajas") de los posibles ciberataques en varias etapas antes de atribuirlos a cualquier actor y antes de que se conviertan en una verdadera crisis.

A partir de este análisis, Darktrace predice que en el 2022, veremos a los actores de amenazas insertar software malicioso en toda la cadena de suministro de software, incluyendo el código fuente propietario, los repositorios de desarrolladores, las bibliotecas de código abierto y más. En consecuencia, es probable que veamos más ataques a la cadena de suministro contra plataformas de software y nuevas vulnerabilidades publicitadas.

Explicando el cambio

Es probable que el aumento de ataques a este sector se deba a que cada vez más empresas dependen de terceros proveedores de confianza para manejar sus datos mientras están en movimiento y en reposo. Este vector de ciberataques ha demostrado ser muy rentable para los atacantes que centraron sus esfuerzos en organizaciones relacionadas para llegar a las joyas de la corona de un objetivo. Este cambio significa que las pequeñas y medianas empresas tienen ahora más probabilidades de sufrir un ataque, aunque no sean el objetivo final.

Recientemente, la vulnerabilidad descubierta "Log4Shell", insertada en una biblioteca de software muy utilizada, dejó expuestos miles de millones de dispositivos y llevó a la Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA) de los Estados Unidos a proporcionar una orientación formal. Desafortunadamente, muchas de estas bibliotecas sólo se actualizan y reciben apoyo de voluntarios, lo que facilita que se cuelen vulnerabilidades y corrupciones intencionadas. El DevSecOps será un punto de debate importante en el 2022, ya que las organizaciones están empezando a comprender la importancia de incorporar la seguridad a las

aplicaciones en una fase mucho más temprana del proceso de desarrollo. Los riesgos que presenta la dependencia del código abierto pondrán a los equipos de desarrollo en una posición clave.

Phishing por correo electrónico sigue siendo un método fiable para los atacantes

A pesar de este relevante cambio de objetivos, Darktrace descubrió que el método de ataque más utilizado en el sector informático sigue siendo el phishing. Darktrace observó que las organizaciones del sector se enfrentaron a una media de 600 campañas únicas de phishing por correo electrónico al mes en el 2021. Estas campañas también han madurado en sofisticación, ya que la mayoría ya no contiene un enlace o adjunto malicioso como en el típico correo electrónico malintencionado.

En el 2022, los atacantes seguirán avanzando en sus ataques por correo electrónico para secuestrar la cadena de comunicaciones de forma más directa. Veremos cómo los atacantes secuestran cuentas de proveedores de confianza para enviar correos electrónicos de spear-phishing desde cuentas genuinas y de confianza, así como vimos en la toma de cuentas del FBI en noviembre del 2021.

Los principales ciberdelincuentes utilizarán correos electrónicos "limpios" que contengan texto normal, con mensajes cuidadosamente elaborados para hacerse pasar por un tercero de confianza con el fin de inducir a los destinatarios a responder y revelar información sensible.

Haciendo frente al aumento de ataques

A medida que la cadena de suministro de software mundial se interconecta cada vez más, los gobiernos, las empresas y las organizaciones de infraestructuras críticas corren el riesgo de sufrir una irrupción, no sólo a través de sus proveedores de software y comunicaciones, sino a través de cualquier fallo de seguridad en la extensa cadena de suministro de software mundial.

Ante esta amenaza de ciberseguridad, las organizaciones deben no sólo centrarse en su propia resistencia cibernética, sino también asegurarse de que pueden hacer que sus proveedores de confianza adopten las mejores prácticas de ciberseguridad. No hay una solución mágica para encontrar ataques insertados en sus proveedores de software, por lo que el verdadero desafío para las organizaciones será operar mientras aceptan este riesgo. Este año, al igual que en el 2021, es cada vez más irreal que estas empresas esperen evitar las amenazas a través de sus cadenas de suministro. En su lugar, deben tener la capacidad de detectar la presencia de atacantes después de una irrupción y detener esta actividad maliciosa en las primeras etapas.

Si los atacantes pueden insertarse al principio del proceso de desarrollo, las organizaciones tendrán que detectar y detener al atacante después de que se haya filtrado. Este problema exige una tecnología de ciberdefensa que pueda detectar vulnerabilidades a medida que los actores de la amenaza las explotan.

Esta amenaza refuerza la necesidad de integrar la seguridad en una fase más temprana del proceso de desarrollo y la importancia de contener rápidamente los ataques para evitar una interrupción del negocio. Como estos ataques tienen varias fases, las organizaciones pueden utilizar la IA en cada paso para contener y remediar la amenaza.

***El autor es CTO, Director de Ciberinteligencia & Análisis en Darktrace.**

3 DÉCADAS

eSemanal

NOTICIAS DEL CANAL

SÍGUENOS EN LINKEDIN

/NOTICIASDELCANAL

3 DÉCADAS eSemanal NOTICIAS DEL CANAL

LAS PERSONAS SON EL CORAZÓN DE LA INDUSTRIA 5.0 Y EL GRAN MOTOR DE CRECIMIENTO PARA 2022

*Por David Montoya

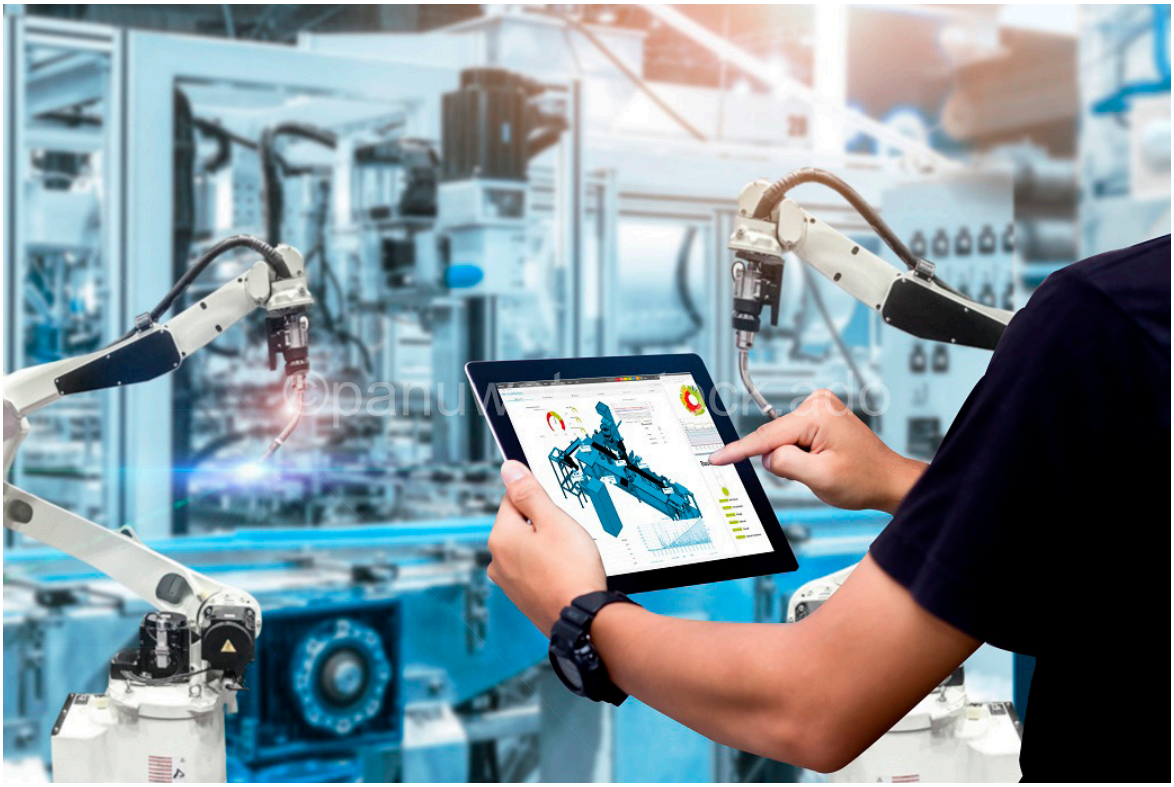
El concepto de Industria 4.0 se afianzó hace un poco menos de una década, y ya algunos visionarios se están centrando en la próxima revolución industrial: la Industria 5.0. Esta revolución tecnológica pretende potenciar la transformación del sector en espacios inteligentes basados en IoT y en computación cognitiva. En este sentido, esta tecnología trata de unir máquinas y humanos para mejorar la productividad y la eficiencia.

La Comisión Europea afirma que los principales objetivos de la Industria 5.0 son la sostenibilidad, el protagonismo humano y la resiliencia, y destaca que la Industria 5.0 ofrece una visión de la industria que va más allá de la eficiencia y la productividad como únicos objetivos, y refuerza su papel y contribución a la sociedad.

La epidemia causada por Covid-19 ha enfatizado el valor de la tecnología en las nuevas dinámicas que tal vez tengamos que mantener. El sector manufacturero ya tenía interés en su transformación digital, sobre todo a través del IoT industrial y la automatización, pero el impacto económico de la pandemia en México nos orienta a visualizar nuevas expectativas en 2022. En México está Industria comienza a ser conocida, primero en el sector manufacturero.

Un estudio de DuckerFrontier y Microsoft afirma que México se encuentra listo para la adopción de esta tecnología en la economía, la sociedad y el mercado laboral, con posibilidades de incrementar el PIB a niveles que van de 4.6% a 6.4% en 2030, por ello, es vital adoptar una mentalidad encaminada a maximizar la adopción de esta tecnología para la automatización de tareas.

contactame@esemanal.mx 55 7360 5651



Para comprender los beneficios que la Industria 5.0 traerá a México en 2022, primero es necesario investigar olas tecnológicas anteriores:

1780 – Mecanización. La primera revolución industrial utilizó el poder del agua y el vapor para mecanizar procesos industriales.

1870 – Electrificación. Esta ola tuvo lugar entre finales del Siglo XIX y principios del Siglo XX. Su punto focal fue la electrificación de fábricas y la creación de líneas de montaje para la producción en masa de productos.

1970 – Automatización. Las primeras tecnologías digitales, incluidos los robots, comenzaron a automatizar tareas que antes realizaban los humanos. Con Internet se produce también la globalización de los procesos productivos.

2011 – Conexión. Comenzó en Alemania, donde el concepto de Industria 4.0 empezó a conectar todo, desde robots hasta automóviles. Es la era de la convergencia entre OT y TI y la reducción de la intervención humana. Uno de los más destacados es IoT e IIoT, con sensores conectados a redes basados en recursos de Inteligencia Artificial.

2020 – Industria 5.0. Al colocar a las personas, ya sean clientes o empleados, en el centro de la producción industrial, la Industria 5.0 ofrece productos diferenciados al mercado y, a los trabajadores, oportunidades laborales destinadas a preservar la vida y el planeta.

El gran diferencial de la Industria 5.0 con relación al modelo 4.0 es que el ser humano está en el centro de esta ola. En este nuevo mundo, los sensores recopilan datos y las computadoras con capacidades de Inteligencia Artificial procesan y analizan esta información. Las máquinas y los robots comienzan a utilizar estos datos y algoritmos para respaldar decisiones que encarnan valores como la prosperidad, la sostenibilidad, la ética y la preservación de la vida.

Los profesionales colaborativos y los robots trabajan codo con codo

En este nuevo paradigma, los profesionales de las plantas trabajarán codo con codo con los robots colaborativos (robots colaborativos o "cobots"). El gestor humano actúa como "coach" del recurso digital, velando por que se sigan los valores humanistas, la preservación del medio ambiente ecológico, la ética y la justicia.

Si bien las máquinas seguirán realizando trabajos peligrosos y repetitivos, las personas utilizarán su cerebro y sus sentimientos para tomar decisiones de alto nivel. Hay un fuerte énfasis en la investigación y los proyectos innovadores que preservan la vida. Una de las tecnologías más utilizadas en la Industria 5.0 es el "Digital Twin", una copia virtual

de una fábrica o una línea de ensamblaje donde se realizan las más diversas simulaciones, incluida la seguridad personal y de propiedad, antes de que se construya efectivamente el piso de la fábrica.

El mercado mundial de 'gemelos digitales' se valoró en $3,800 millones de dólares en 2019 y se espera que alcance los $35.800 millones de dólares en 2025. Según el análisis de Gartner "IoT Digital Twin Adoption Proliferates Across Many Sourcing Options", la adopción de gemelos digitales es paralela a la del Internet de las Cosas (IoT): 26% de los encuestados afirma haber implementado ya gemelos digitales, y 59% está implementando o planea implementarlos en el próximo año.

Para que estos logros sucedan, se están gestando cambios. Se formarán nuevas asociaciones estratégicas entre el 40% de los principales proveedores de TI y OT en el mercado global. El objetivo es llegar a una solución holística que reduzca los costos de integración e implementación en un 20 %. Habrá un aumento del 40 % en las inversiones en gobernanza de datos, equipos de ingeniería digital y tecnologías de operaciones digitales.

También será necesario invertir en una cultura centrada en productos y servicios altamente individualizados. Para ello, las organizaciones están equipando sus productos industriales con componentes y sensores digitales. Esto facilitará que los productos se comuniquen entre sí, reciban señales y utilicen tecnologías como 5G y LoRaWan. Los componentes de IIoT crean una visión más transparente del estado de productos individuales y procesos completos y, por lo tanto, permiten una intervención rápida en casos de dificultades inminentes (gestión predictiva).

El monitoreo de 360º cumple con los estándares ESG

El enfoque humano de la Industria 5.0 requerirá que los directivos tengan una visión 360º del siempre heterogéneo entorno industrial y, a partir de ahí, poder implementar continuamente innovaciones y optimizaciones. Cuanto más transparente sea la visión que el gestor tenga del entorno, mayor será la eficiencia y más cercano el cumplimiento de los valores ESG (medioambientales, sociales y de gobernanza). Por supuesto, la Industria 4.0, la modernización y la interconexión entre TI y OT también requieren la expansión del monitoreo. El objetivo es proteger los procesos interdepartamentales y revelar interrelaciones críticas.

Además de lograr una visión predictiva de todo lo que sucede en la Industria 5.0, existe otro frente de batalla para avanzar en este concepto: la falta de profesionales preparados para este universo.

México y el mundo sufren la escasez de profesionales capacitados para las nuevas olas tecnológicas. En 2022, por lo tanto, será más importante que nunca automatizar tantos procesos de TI y OT como sea posible para que los recursos humanos se utilicen para la innovación y transformación empresarial, no para procesos repetitivos. La escasez de habilidades destacará a los MSP (Proveedores de Servicios Administrados) mexicanos que ya tienen equipos formados en la Industria 4.0 y ahora se están moviendo hacia la era de la Industria 5.0. Hay espacio para MSP especializados en sectores específicos como en sectores automotriz, industria química, etc.

Sin duda, hay un gran reto de formar profesionales para la Industria 5.0. Para que estos logros se lleven a cabo, es fundamental repensar el modelo pedagógico en Mexico. Las habilidades necesarias para acompañar la Cuarta y Quinta Revoluciones Industriales solo tendrán efecto si se equilibra el déficit educativo de la población acorde con la demanda empresarial.

No se pueden saltar pasos

La Industria 5.0 con sus valores éticos, inclusivos y sostenibles solo sucede donde la Industria 4.0 ya se ha implementado antes. El profesional alineado con la Industria 5.0 será más calificado, habrá estudiado más años y estará acostumbrado a una rutina de renovación continua de sus conocimientos. Es fundamental que, en 2022, haya incentivos para que se implemente este cambio de paradigma y llegue el nuevo.

***El autor es Director Global de Desarrollo de Negocios de IoT en Paessler.**

DELL PRESENTA NUEVOS EQUIPOS PARA IMPULSAR LA COLABORACIÓN Y AUMENTAR LAS EXPERIENCIAS VISUALES

Redacción eSemanal

• LA XPS 13 Y EL MONITOR ULTRASHARP, LOS NUEVOS PRODUCTOS QUE ENGROSAN EL PORTAFOLIO DE LA MARCA.

• CON CARACTERÍSTICAS QUE AMPLIFICAN LA EXPERIENCIA VISUAL Y LA COLABORACIÓN, EL FABRICANTE APUESTA POR ESTOS DOS RUBROS EN 2022

Inició el 2022 y Dell Technologies lo apertura con la presentación de dos equipos, una PC portátil (XPS 13) y el nuevo monitor de 32 pulgadas con resolución 4K, los que además de abrir oportunidades de negocio para los canales, llevarán la colaboración y las experiencias visuales un paso más adelante.

En el marco del CES 2022, el fabricante dio a conocer los nuevos hardware que se suman a su portafolio, destacando la portátil Dell XPS 13 Plus, de la cual se dijo que está inspirada en la generación Z, al ser moderna, con estilo, accesible y eficiente; no obstante, su estética no disminuye su performance, ya que cuenta con un procesador Intel Core de 12ª generación de 28W (a diferencia de los 15W del anterior), enfriada por ventiladores más grandes que proporcionan un 55% más flujo de aire sin aumentar el ruido o la temperatura.

XPS 13 Plus

La movilidad es una característica de los equipos portátiles y gran parte de ello descansa en contar con una batería que permita la autonomía durante un periodo de tiempo prolongado y tecnología para permitir una carga rápida, es por ello que, la XPS 13 Plus integró la tecnología Express Charge 2.0 que logra hasta un 80% de la carga de baterías en menos de una hora, asegurando su uso sin interrupciones, durante horas de trabajo.

Durante la presentación, también se resaltó el trackpad tradicional que ha sido sustituido por un touchpad de cristal sin bordes que proporciona respuestas al tacto, la resolución en 4K+, pantalla OLED con Eyesafe, altavoces cuádruples y debido a su proceso de fabricación, Dell aseguró que es totalmente reciclable, pudiendo reutilizarse en nuevos equipos y cumpliendo con la iniciativa Objetivos 2030 de Dell Technologies.

Monitor Dell UltraSharp

El segundo producto que la marca develó durante el CES 2022, corrió a cargo del monitor UltraSharp con características como: tecnología de panel IPS Black, cámara web inteligente con sensor Sony STARVIS CMOS 4K HDR que ayudan con los ajustes de luz, capacidad de encuadre automático con Inteligencia Artificial (IA), funciones de seguridad inteligentes integradas, claridad visual, micrófonos de doble matriz con cancelación de eco y altavoces de 14 watts, con el cual busca abrir oportunidades para sus partners en el terreno de la colaboración.

Asimismo, la empresa destacó la certificación del monitor con Microsoft Teams, su estética limpia, sus amplios puertos y sus opciones de conectividad.

TS700-E9-RS8 de
Asus

Servidor/Workstation, con capacidad de expansión y escalabilidad para una amplia gama de aplicaciones de almacenamiento y redes. Admite dos tarjetas gráficas de doble ranura con dos enlaces PCIe 3.0 con soporte para Nvidia Cuadro y AMD CrossFireX. Siete ranuras PCIe para incluir tarjetas adicionales como HAB/ RAID y 10G LAN y hasta 12 memorias DDR4 ECC.

Descripción

Presenta un diseño flexible que se adapta a entornos de oficina y centro de datos, su kit de riel de servidor permite una fácil integración en un servidor de rack de centro de datos.

Características

- CPU 1 x Intel Xeon Silver 4210R
- Memoria 1 x 16GB DDR4, expandible hasta 1.5 TB ECC/ Non-ECC (12 DIMM
- Almacenamiento 1 x 1TB HDD 3.5” Sata Hot-Swap, Bahías disponibles para almacenamiento: 7 x 3.5” Hot-Swap
- 1 x PSU redundante1+1800W 80 plus platinum
- Módulos de expansión 7 x PCIe Gen3 x16 (3 x Gen3 x16 + 2 x Gen3 x16/Gen3 x8 + 2 Gen3 x8)
- LAN 2x LAN 1 GbE Intel I210-AT

Disponibilidad

Abasteo.

contactame@esemanal.mx

ZX10 de
Getac

Tableta de 10” con SO Android 11, procesador Qualcomm Snapdragon 660 y GPU Adreno 512. Ofrece un flujo de trabajo eficiente para profesionales de seguridad y servicios públicos, energía, transporte y logística, fabricación y automoción.

Descripción

Rugerizada, tiene 17,9 mm de grosor y un peso de poco más de 1 kg. Las certificaciones MIL-STD-810H e IP66 acreditan que puede resistir caídas de hasta 1,8 m, golpes, lluvia, vibración, polvo y derrames líquidos. Además, su rango de temperatura operacional de -29 °C a 63 °C (-20 °F~145 °F).

Características

- Cámara frontal de 8 MP y posterior de 16 MP
- GPS específico
- Ranuras dobles para tarjetas SIM LTE
- Dos baterías intercambiables en caliente
- Opciones de hasta 6 Gb de memoria RAM LPDDR4 y 128 Gb de almacenamiento
- Pantalla LumiBond de visibilidad a la luz solar (con 800 nits de brillo), resiste lluvia y responde al tacto con guantes
- Micrófonos dobles filtran los ruidos fuertes de fondo
- Wi-Fi 802.11 ac, Bluetooth (v5.0) y módulo LTE 4G opcional
- Disponible con aplicaciones específicas que combinan diferentes características, accesorios y servicios de software
- Disponible en marzo 2022

contactame@esemanal.mx


3 DÉCADAS
eSemanal
NOTICIAS DEL CANAL
Manténte Cerca
SÍGUENOS EN
revista_esemanal
www.esemanal.mx

3 DÉCADAS eSemanal
NOTICIAS DEL CANAL

MANTENTE INFORMADO EN NUESTRAS REDES SOCIALES