Año 2. Número 6.

Bridge

CISCO SECURE

Ciberseguridad

Especial Trabajo híbrido

CX Danilo Pozo

VP Customer Experience, Cisco

Quién es quién: Luz María Murguía

OCP TECH

INGENIERÍA DE **IMPACTO**

EXPERTOS EN SOLUCIONES DE CIBERSEGURIDAD

¡CONOCE MÁS DE OCP TECH!

OCP TECH
OCP . TECH

CISCO Partner

ARGENTINA

Ing. Enrique Butty 240
piso 3 Capital Federal,
Buenos Aires, Argentina
T +54.11.2152.9600

COLOMBIA

Cra 9 N0. 115-06 Piso 7
Of 701, Edificio Tierra Firme,
Bogotá, Colombia
T +57 1 442 3209
T +57 313465.3030

USA

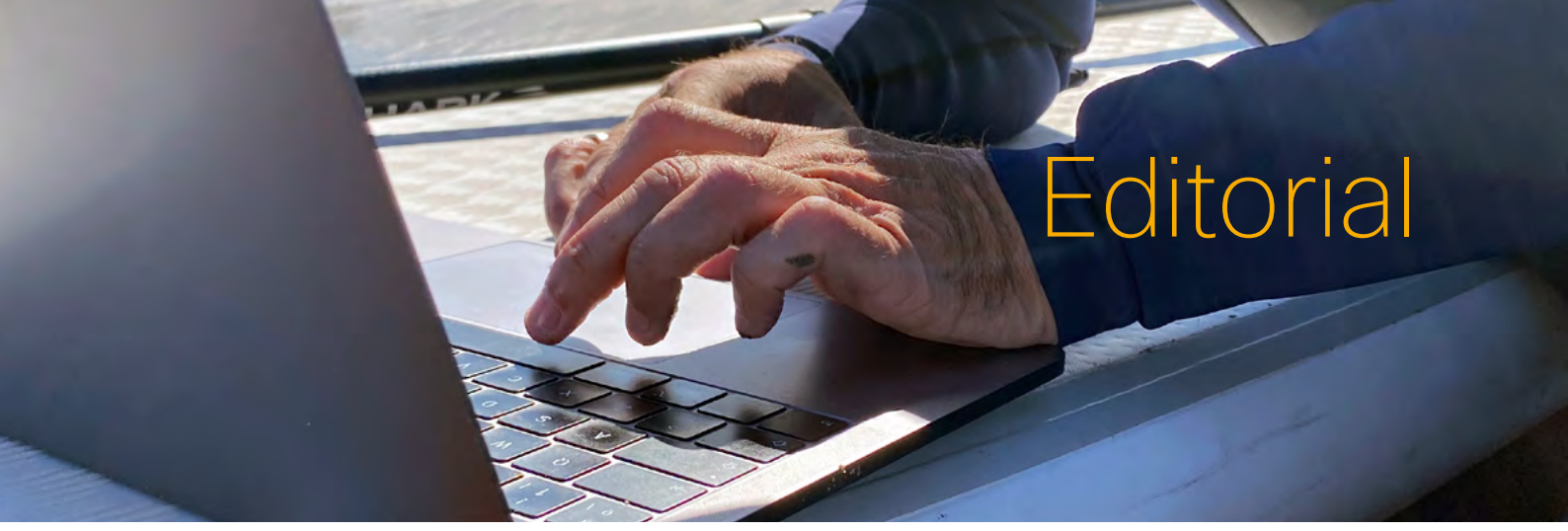
333 S.E. 2nd Avenue, Suite
2810, Miami, Fl 33131
United States of America
T +1.305.537.0800
T +1.305.537.0704

PANAMÁ

Oceania Business Plaza
Torre 2000 Piso 33 A,
Boulevard Pacífica - Punta
Pacífica, Panamá City -
República de Panamá
T +507 3877300

PERÚ

Calle Las Orquídeas 585,
Edificio Fibra, pisos 12 y
13, San Isidro, Lima.
T +511 712.5901



Editorial

Trabajar desde la playa podría interpretarse como la máxima expresión del trabajo remoto, de la libertad, del "work life balance". También desde una mirada negativa se podría pensar que la persona no puede dejar de trabajar ni siquiera en sus vacaciones. Desde el equipo editorial de Bridge, por supuesto, nos quedamos con la primera impresión.

A lo largo de esta edición recogemos perspectivas que sustentan el trabajo híbrido como modelo a seguir desde la convicción de que es la respuesta que buscan los trabajadores para equilibrar su desempeño en la vida, y también los empleadores, desde una lógica de productividad y retención de talento.

Estamos ante un cambio de época. La pandemia fue un catalizador de transformaciones que se venían gestando desde hace tiempo. Como señala nuestro columnista Pablo Marrone "la pauta cultural fluye, como si fuera un reloj de Dalí". Ese reloj distorsionado, maleable, nos hace pensar en una disrupción en el tiempo, en los horarios, en la sincronía, un cambio fundamental en la manera de interactuar socialmente, de colaborar, de hacer las tareas.

Poder gestionar este cambio individual y colectivamente supone un gran desafío. Hace casi diez años, el filósofo Byung Chul Han nos advertía casi premonitoriamente sobre un futuro distópico en su libro "La sociedad burnout". Allí describe la fatiga como "la enfermedad de la sociedad neoliberal del desempeño" en la que "voluntaria y entusiastamente nos explotamos a nosotros mismos en la convicción de que nos estamos realizando". Luego en otro de sus trabajos el mismo autor nos hablaría del "Aroma del Tiempo" y de "La Desaparición de Los Rituales". Parece que el filósofo viene entretejiendo los argumentos fundamentales para un llamado a reflexionar sobre la necesidad de cambio en nuestro *modus vivendi*.

Una buena implementación del trabajo híbrido es seguramente parte de la respuesta a la necesidad de explotar nuestras capacidades de producción en un sentido positivo, en lugar de explotarnos a nosotros mismos.

Personalmente me resisto a una mirada superficial sobre los beneficios del trabajo híbrido desde una lógica de productividad acotada al ahorro de tiempo o de la preferencia por la comodidad de trabajar en pijamas. En cambio, creo que el panorama actual nos enfrenta a la posibilidad de diseñar el trabajo de esta nueva era, creando los ambientes de productividad más efectivos para cada perfil de colaborador, entendiendo la productividad como debe ser: producir los mejores resultados, propiciando el mejor desempeño cognitivo, y esto se logra cuando las personas están motivadas, energizadas y se encuentran en un fluir más armonioso entre el trabajo y la vida personal, en otras palabras, en un "work life flow".

Juan Marino

Staff

Producción Integral
Basanta Contenidos

Directora Editorial
Karina Basanta

Director de Arte
Nicolás Cuadros

Coordinadoras
Marta Pizzini
Marta Assandri

Producción audiovisual
Salpufilms

Colaboran en este número
Silvia Montenegro
Jorge Prinzo
Freddy Macho
Pablo Marrone

Fotografía e ilustración
Basanta Contenidos
Freepik
Pixabay
Unsplash

Agradecimientos
Nicolás Cacciabue
Isabella Cacciabue
Jorge Cuadros
Joaquín Cuadros
Santino Cuadros

Foto de Tapa
Basanta Contenidos

Directora Editorial
Karina Basanta

Director de Arte
Nicolás Cuadros

Impresión: FP Impresora
Antonio Beruti 1560, Florida Oeste,
Provincia de Buenos Aires
Tel: 11-4760-2300
www.fpimpresora.com.ar

basantacontenidos.com
basanta@basantacontenidos.com
@basantacontenidos
+54 911 5014-4510 / 5260-8723

Ilustración: Freepik.

Revista Bridge **Impresa / Digital**
Año 2. Número 6

Cisco Latinoamérica

Cyber Security Director,
Americas Service Providers
and Latin America at Cisco
Ghassan Dreibi

Líderes Regionales de Ciberseguridad

Juan Marino
Fernando Zamai
Juan Orozco
Yair Lelis
Marcelo Bezerra

Editor General
Juan Marino

Agradecimientos
Taiane Belotti
Luz María Murguía
Danilo Pozo
Jackeline Carvalho
Militza González

Marketing

Taiane Belotti
Líder de Marketing, Seguridad Latam
Jimena Reyna Briseño
Gerente de Marketing de Contenidos, Seguridad, Latam

Bridge Nº 6

Sumario

OFFICIAL TECHNOLOGY PARTNER

Cisco y Real Madrid unidos para crear el estadio más conectado de Europa.

Como Partner Tecnológico Oficial del Club, Cisco equipará al nuevo estadio Santiago Bernabéu con un despliegue integral de su tecnología líder en la Industria. La actualización incluirá soluciones de conectividad, seguridad, centros de datos y señalización digital, todo ello diseñado sobre una única red inteligente y convergente de Cisco.

El estadio multiusos de 85.000 asientos contará con la mayor red de conectividad inalámbrica basada en tecnología Wi-Fi 6 de Europa.

Más de 1.200 puntos de acceso Wi-Fi 6 en el Santiago Bernabéu ofrecerán una comunicación segura con mayor velocidad, fiabilidad y ancho de banda que el anterior estándar Wi-Fi para que los fans disfruten de experiencias más inmersivas al interactuar con sus dispositivos y aplicaciones a través de la emisión y repetición de fotos y videos.

En el transcurso de los próximos años, la conectividad remodelará la industria del deporte y redefinirá lo que es posible.

Creemos que la digitalización es más importante que nunca.

Juntos, Cisco y Real Madrid llevan al sector del deporte y el entretenimiento hacia el futuro y más allá.

En la Visión de

Taiane Alves
Líder Marketing de ciberseguridad, Latinoamérica, Cisco.

En los últimos años se hizo evidente el crecimiento del SaaS como estrategia de negocio y se va por más. ¿Cómo acompaña el departamento de marketing esta tendencia?

Es un desafío muy grande, ya que el sector SaaS (Software as a Service) crece cada año. Según un informe de Gartner, se trata de un mercado que se espera genere alrededor de US$ 85,1 mil millones en 2022 y alcance un total de US$ 113,1 mil millones en 2023, es decir que aporte un crecimiento de 32,9% en solo un año.

En un escenario de intensa competencia y alta tecnología no hay espacio para hacer todo a la antigua. En otras palabras, las soluciones surgen a una velocidad cada vez mayor y con funciones específicas para resolver los problemas de las corporaciones, por lo que no es inteligente perder tiempo (y dinero) tratando de conectar estos sistemas manualmente.

De esta forma, para estar a la altura del sector, destacar entre la multitud de competidores y abrazar este espacio de oportunidades, es imprescindible contar con una estrategia de marketing bien orquestada, enfocada en lo digital, esto se vuelve crucial y obligatorio para el éxito de una campaña de marketing. Cuando hablamos de software como servicio, por no ser un producto físico y tangible, debemos ir más allá de las tácticas de marketing convencionales. Algunos elementos que deben acompañar al mercado SaaS con el objetivo de atraer nuevos clientes y generar negocios son: campañas 100% digitales, marketing de contenido, inversión en optimización SEO, ofertas de prueba gratuitas, experiencia del cliente, uso de CTA's (call to action) atractivos y claros y todo esto combinado con un plan continuo para la retención de clientes a largo plazo.

En Cisco esta migración se ve acompañada por una fuerte estrategia de CX (Customer Experience). ¿Cuál es tu visión de esa doble corriente, es decir, dónde ves el punto de unión?

Diría que hay más de un punto de unión. Es casi imposible pensar en una estrategia de marketing enfocada en SaaS sin pensar en la experiencia del cliente. El viaje de compra, desde la experimentación del producto hasta la compra real, debe diferenciarse. El cliente necesita tener un trayecto sin percances ya que el modelo SaaS solo prosperará con el cliente satisfecho. Si por alguna razón el usuario tiene una mala experiencia, simplemente cambiará a otra solución de la competencia. En resumen: la estrategia CX es esencial para el marketing de SaaS.

Esta edición de Bridge está atravesada por la modalidad de trabajo híbrido desde distintos puntos de vista. ¿Cuál es el del departamento de marketing de Ciberseguridad de Cisco Latam?

Para hablar de trabajo híbrido es importante señalar cuál es su significado. En mi opinión, el trabajo híbrido es mucho más que el simple hecho del lugar donde se ejerza -ya sea en casa, *coworking* o sede de la empresa-, sino la oportunidad de darle al empleado el poder de elección. Poder elegir el lugar desde donde trabajar va mucho más allá del trabajo en sí, también da libertad y autonomía con beneficios positivos en la productividad, la calidad de vida y el bienestar de las personas. Por supuesto, el tema de la ciberseguridad es importante cuando trabajamos de forma remota, pero siempre creo que el sentido común y las soluciones de protección adecuadas, junto con una política de seguridad de la información de la empresa, brindarán la tranquilidad de poder realizar la función desde cualquier lugar.

Pregunta **abierta**

Esta sección se llama Pregunta Abierta porque invita a la entrevistada a generar su auto pregunta con tema libre. ¿Cuál es la tuya? ¿Y tu respuesta a ella?

Me gustaría compartir algunos resultados del "Informe de seguridad Duo" de Cisco, que revela el aumento en el uso de soluciones MFA (autenticación de factor múltiple) en empresas que han adoptado el trabajo híbrido. A continuación les comparto algunos números de este reporte:

- La autenticación multifactor ha aumentado a medida que las empresas dejan de usar contraseñas para proteger a los trabajadores híbridos.

- La biometría ha aumentado significativamente, con un crecimiento del 48 % en las autenticaciones respecto al año anterior.

- Más de la mitad de los tomadores de decisión de TI planea implementar una estrategia sin contraseña.

- Duo también ha visto un crecimiento de cinco veces en el uso de autenticación web (WebAuthn) desde abril de 2019.

- América Latina tuvo un crecimiento del 18% en el uso de autenticación a través de aplicaciones en la nube. Europa y Medio Oriente tienen el porcentaje más alto, con 190%.

La autenticación sin contraseña de Duo es parte de la plataforma Zero Trust, líder en el mercado de Cisco, que protege el acceso de cualquier usuario, desde cualquier dispositivo y en cualquier aplicación o entorno de TI. El producto está diseñado para ser independiente de la infraestructura, lo que allana el camino para un futuro sin contraseñas al tiempo que garantiza que las corporaciones puedan asegurar cualquier combinación de aplicaciones en la nube y locales, evitando brechas de seguridad graves.

Te dejo aquí la invitación para que descargues Duo (prueba gratis) hoy: https://signup.duo.com/trial

Imagen: Gentileza Taiane Alves.

Testimonios de éxito

Networking Academy

En primera persona

Rafael La Selva,
Ingeniero en Sistemas
de Cisco, Dynalogic.

por **Rodolfo Basanta**

¿Qué te motivó a unirte al programa de ciberseguridad de NetAcademy?

En agosto de 2017 recuerdo haber leído un artículo en un blog de noticias donde Cisco estaría ofreciendo capacitación en Seguridad Cibernética para quienes se inscribieran; el número estaba limitado a 10.000 postulantes para una de las primeras clases. Este fue el primer contacto que tuve con el programa de NetAcademy. En ese momento, ya estaba trabajando como ingeniero de posventa de seguridad y, como estaba familiarizado con el portafolio de Cisco, decidí postularme. Me aprobaron con éxito y al final pude solicitar otra certificación técnica con un comprobante proporcionado por Cisco.

¿Cómo fue tu experiencia allí?

Fue un viaje agradable, aproximadamente 6 meses de mucho aprendizaje y práctica. No fue solo un curso, sino una verdadera capacitación con todo el apoyo de la comunidad y los colegas. Con el programa de becas y NetAcademy de Cisco pude continuar desarrollando mis habilidades y mi carrera en virtud de convertirme en un profesional más completo y apegado a las exigencias del mercado, especialmente en Ciberseguridad.

Estás trabajando en Dynalogic. ¿Cómo contribuyó tu formación a ello?

La educación es sin duda un punto fundamental en la vida de cualquier persona, tengo una carrera y algunas certificaciones que me dieron una buena base, además de una amplitud sin fronteras para el mercado de TI e Infraestructura. Recuerdo que ya en el primer semestre de la universidad conseguí mi primer trabajo como pasante donde pude llevar a la práctica todo lo aprendido durante el curso. Poseer un segundo o incluso un tercer idioma sigue siendo esencial para ampliar horizontes.

Sin embargo, creo que mucho más importante que el conocimiento es el viaje. El acceso a grandes líderes y mentores, colaborar en casos con equipos experimentados que conocen del tema fue lo que realmente me ayudó a obtener la dirección y el enfoque necesarios para mi desarrollo técnico e interpersonal.

El mercado indica que existe una gran demanda de expertos en ciberseguridad. ¿Cuál es tu recomendación para cualquiera que busque desarrollo profesional?

Puedo decir que esta es una alerta que viene llamando la atención y que escucho desde hace años y desde que todo apunta a la aceleración de la digitalización. Además, la demanda de ciberseguridad acompañó a este movimiento desde que la personas de todo el mundo pueden acceder a internet desde sus propios "dispositivos". Por ejemplo, hoy en día ya es normal que los empleados puedan trabajar desde casa con sus portátiles personales o de la empresa, o incluso acceder a directorios y archivos sensibles desde fuera de la organización desde su smartphones y tablets. Al observar estos escenarios, puede imaginarse el desafío de hacer que todos estos dispositivos y accesos sean seguros. Por ello ha cobrado tanta importancia la búsqueda de profesionales especializados en ciberseguridad, ya que nos encontramos en un contexto aún más hostil que en el pasado dada esta movilidad y descentralización de los datos.

Para todos aquellos que buscan desarrollarse profesionalmente en ciberseguridad hay muchas oportunidades: capacitarse, aprender y evolucionar en el camino, exponerse a situaciones críticas y trabajar colaborativamente con grupos más experimentados. Estoy seguro que con el tiempo las respuestas a muchas de las preguntas vendrán naturalmente

Basanta
contenidos

Contenidos Multiplataforma

basantacontenidos.com

Producimos contenidos originales

Entrevista

Danilo Pozo
VP Customer Experience,
Cisco.

CX

Imagen: Youssef Naddam, Unsplash.

Custodiar y promover una experiencia de cliente óptima es uno de los objetivos más importantes de las organizaciones de hoy. En un contexto de alta competencia donde cualquier falla puede desencadenar en la pérdida de un usuario, el área de CX toma un rol clave. Tanto que toda la cultura organizacional precisa encolumnarse a ella. Para profundizar en este tema hablamos con Danilo Pozo, VP de CX, Cisco.

por **Karina Basanta y Jorge Prinzo**

¿De qué hablamos cuando hablamos de Customer Experience? ¿Cómo nace este concepto? Es algo que debería haber existido siempre, sin embargo en la era digital cobra una relevancia que antes quedaba solapada.

Cisco siempre ha estado atenta al negocio del cliente; una de las cosas más lindas de la empresa es que ve a la gente como una prioridad. Creo que Customer Experience nace de cómo tenemos una metodología, un proceso, cómo armamos un equipo para asegurarnos de que ese sentimiento, esa percepción que el cliente tiene sobre cómo puede crecer con Cisco, tenga una vía que le permita lograrlo. Además, entender cómo el cliente está creciendo en su transformación digital. Todos estamos bajo una tremenda presión para entregar valor de una forma más fácil, para llegar al mercado más rápido. Customer Experience tiene como objetivo custodiar la experiencia del cliente con Cisco y acompañarlo a que cumpla sus metas. Obviamente, trabajando con el partner en conjunto para potenciar el valor de ambas empresas y llevar una única solución hacia nuestros usuarios, a fin de que estén conectados de una forma mucho más veloz, más ágil, más segura... trabajar juntos para incrementar la automatización y el uso de inteligencia artificial, para que la operación sea más dinámica y pueda tener resultados más rápido.

¿Cómo se mide la experiencia del cliente? ¿Hay alguna plataforma específica para ello? ¿Qué es el RoX?

Pues sí. Nosotros tenemos tres cosas que son sumamente importantes, que son nuestro norte, nuestra visión. Primero, lo que llamamos CX Lifecycle, que es básicamente la metodología de cómo nos alineamos desde Cisco con el cliente, con el partner para asegurarnos tener no sólo el mejor portafolio, sino también los expertos y los procesos adecuados para que se implemente de una forma rápida. Luego, adentrándonos en la fase de compra, buscamos asegurar que el camino sea más fácil, ágil. Esto nos lleva a lograr una integración óptima que garantice la implementación en el momento y en el lugar más adecuados para las necesidades del cliente. Y lo que estamos comenzando a sumar y a desarrollar de una manera más fuerte, es la parte de adopción de tecnología. Y eventualmente, llegar a que el mismo cliente comience a distribuir la noticia de que Cisco tiene una solución robusta, rápida y segura. A su vez, en Cisco, a partir de la vivencia de los usuarios, renovemos esa plataforma y la expandamos para lograr el Return of Investment o Return of Experience.

Nuestro segundo *aproach* es que todo viene alrededor de *insights* en telemetría. A mí me gusta decir que CX está en el negocio de las personas (*People Business*), pues nuestro equipo no crea un servicio o un producto. Nosotros vemos cómo la gente trabaja con Cisco, cómo percibe a la empresa y a sus soluciones. Esto está basado en datos y telemetría, y tiene que ver específicamente con la combinación de las plataformas digitales. Hoy trabajamos con lo que llamamos CX Cloud, que es un un portal, que nos da la oportunidad de ver dónde está la plataforma del cliente, dónde está su red, qué tan vulnerable puede ser, qué tan segura está, cuáles son las versiones de software que tiene, qué le conviene. Es muy dinámico, y nos permite acelerar al cliente y llevarlo de un estadio al siguiente, a través de sesiones web que le ayudan a entender qué compró, cómo utilizarlo, cómo adoptarlo.

Y lo último que medimos es el éxito del portafolio de Cisco. Lo que CX busca hoy es no solamente crearlo y ofrecerlo sino escuchar al cliente para saber qué está experimentando con él. Especialmente alrededor de lo que llamamos Success Tracks y Business Critical Services, que son combinaciones de servicios y de adopción que le ayudan al cliente en arquitecturas específicas a acelerar el uso. Y escuchar, dentro de todos los niveles que tenemos en esas dos plataformas, cuál es el nivel adecuado para el cliente, no sólo para servicios, sino también para el software, la combinación de las soluciones.

Se me ocurre que Customer Experience está atravesando todas las verticales, porque se mira la satisfacción del cliente en todas: seguridad, arquitectura, redes. No es que este departamento es independiente, sino que es transversal a todos.

Sí. Yo creo que uno de los valores más importantes que tenemos como empresa es el multidominio, la habilidad de tener un portafolio vasto, amplio. Si hablamos por ejemplo de colaboración, nos ocuparemos de qué tan rápida pueden tenerla nuestros clientes, nuestros partners o nosotros mismos internamente, de cómo la consumimos. Pero también, dentro de esa plataforma de colaboración, pondremos foco en otros ingredientes muy importantes: seguridad, estabilidad de la red, agilidad, rapidez y claridad que pueden tener los servicios. Entonces creo que uno de los valores más grandes de Cisco como empresa es esa habilidad de contar con multidominio, multiplataforma, y que se complementen. Tienes toda la razón; parte de nuestro valor agregado es asegurarnos de que nuestro cliente acceda a ese portafolio vasto y ayudarlo en su crecimiento.

¿Cómo se toman los *insights*? Seguramente una parte se alimenta de las métricas de CX Cloud, por ejemplo. Pero adicionalmente, cuando el cliente habla, más allá de lo que sucede con la plataforma, ¿a través de qué medios se expresa? ¿A través de su ejecutivo de cuenta, a través de Soporte...?

Hay una combinación de mucho, y lo que acabas de decir es todo correcto. Lo primero que nosotros hacemos es poner *appliances* y/o productos que nos den esa telemetría. Uno de ellos es el que llamamos Compass, una herramienta para obtener toda esa data de parte del cliente, que es totalmente dinámica y proactiva. Sin embargo, una vez recibida esa información, ¿qué se hace? Si tenemos un reporte con información, y no logramos traducirlo al idioma del cliente, no tiene el valor que nosotros queremos, o que el cliente mismo quisiera que tuviéramos. Dentro de cada cuenta de grandes clientes, que son organizaciones que adoptaron niveles de software y de servicios importantes, tenemos lo que llamamos Customer Success Executives, que son los que están específicamente dedicados a uno o dos clientes como máximo. Ellos son los encargados de traducir esa información para asegurarnos de que el cliente tenga la noción de dónde estamos, dónde queremos estar y adónde vamos, qué tan rápido podemos llegar juntos. Porque, recuerda: todo se trata de ver cómo optimizamos los retos que tenemos hoy, cuáles son y cómo aceleramos los retos que va a tener el cliente mañana, y al final, cómo innovamos con *pictures* que podamos definir en conjunto con el cliente. Entonces, tenemos esa combinación de telemetría por medio de reportes específicos basados en su red, con *appliances* y productos que instalamos con ellos y nuestros *partners*, y tenemos también el *insight* de discusiones con nuestro ejecutivo. Cuando no contamos con Customers Success Executives, trabajamos muy de cerca con nuestros socios de negocios a través de lo que llamamos Success Program Managers, que ya tienen muchos clientes, pero también están midiendo la adopción del Lifecycle.

Entonces es una combinación, cuando decimos que estamos en el *People Business* es con la data, pero traduciéndola al lenguaje que quiere el cliente y a dónde queremos llegar.

Pensaba en la estrategia de negocios; siempre se piensa en vender, y también se piensa en fidelizar. Me parece que tiene que haber un equilibrio, como si fueran dos platillos de una balanza, y el punto de equilibrio es la experiencia del cliente, porque al vender más sin pensar en cómo retener a ese cliente, sin que se sienta satisfecho, no hay equilibrio.

Cien por ciento de acuerdo. Y te digo una cosa. Personalmente, tengo toda mi carrera en Cisco basada en Ventas; llevo en la empresa veintiún años, y de ellos he pasado dieciocho años en Ventas. Y esta es la primera oportunidad que tengo de estar en una organización donde la venta, que siempre es importante, no se da por una propuesta, sino que se da por medio del valor que entregamos, y cómo expandimos una renovación. Ningún cliente va a expandir una renovación si no tuvo una experiencia excelente con la solución, con la gente con la que trabajó y con la metodología y el proceso. El cliente va a comprar y extender esa venta basado en cómo CX trabajó con él lado a lado. Entonces hoy, lo que nos da el éxito es cómo el cliente percibe a Cisco íntegramente, no solamente al área de Servicios o de Software. En Latinoamérica tenemos resultados muy buenos y positivos. Una de nuestras métricas está dada por lo que llamamos CX Sat, aporta la satisfacción que tiene el cliente basado en el trabajo que venimos haciendo en el área de servicios, *delivery*, o entrega de nuestra expansión de renovaciones. Éstas son datas métricas importantes para entender cómo vienen las siguientes, que llegarán con el Renewal rate: qué tan rápido, que tan a tiempo lo están haciendo los clientes; y todo el proceso de Lifecycle y de adopción que estamos creando. Entonces, te diría que hoy la venta es importante, pero no es lo que nos dice el factor de éxito. Por eso Laércio Albuquerque (VP Latin America, Cisco) y yo trabajamos coordinadamente y en conjunto, porque el resultado que él tiene, tiene impacto en el nuestro, y el nuestro tiene impacto en el de Ventas. Ahora, nuestra discusión con el cliente no está basada en la pregunta de toda la vida: ¿cómo te puedo ayudar?; ya sabemos cómo le podemos ayudar. Hoy tenemos la información, podemos decirle "esto es lo que está pasando, estos son los comportamientos que estamos viendo, y éste el valor que te podemos traer basado en nuestra arquitectura y en nuestro portafolio".

Te escucho hablar, y pienso que ustedes se anticipan. Por lo general, sucede que a las empresas les pasa al revés: el cliente primero se queja, o primero pide; en realidad aquí está la posibilidad de anticiparse a la necesidad, de proponerlo primero.

Correcto. Básicamente, nuestro modelo es tratar de adelantarnos a los eventos, tratar de entender bien cuáles vienen. No solamente hablamos del comportamiento de la red, porque siempre ha sido una de nuestras prioridades, sino también desde el punto de vista de negocios: cómo nosotros incubamos los negocios que son importantes, cómo nuestro portafolio encaja en lo que es importante para ellos. Porque no es simplemente esa filosofía de que vas a vender lo

Imagen: Diego ph, Unsplash.

que está, eso ya no funciona; tienes que ver qué está en esa plataforma, pero cómo lo combinas con las prioridades que el cliente tiene.

Pensaba también en la capacitación, porque imagino que toda la organización tiene que estar alineada pensando en este objetivo: no solamente en hacer crecer el negocio con ventas, sino también en sostener esa satisfacción absoluta en el cliente.

Sí, estamos de acuerdo en el ciento por ciento. Comenzamos este proyecto hace tres años y medio, y es muy lindo construir y verlo crecer, porque comienzas a ver las capacidades que tienes como compañía y cómo tu equipo incorpora gente nueva que aporta una filosofía diferente. Tal como tú dices, en este crecimiento es importante contar con un esquema de entrenamiento que sea bastante robusto. Nosotros hoy tenemos trainings elaborados para distintas etapas: Blue, Green y Black belt, por ejemplo; es un currículum bastante extenso, para que nuestra gente, dependiendo del rol que tenga, adquiera ese conocimiento en mucho detalle. Hoy en CX hay cinco roles específicos. Primero está el equipo de Business Development; ellos tienen específicamente entrenamiento alrededor del desarrollo del portafolio. Después tenemos un equipo de Delivery, que atiende lo relacionado a la entrega, la implementación, la migración de nuestra plataforma y la optimización de las plataformas por medio del portafolio de Business Critical Services. Además, contamos con tres equipos importantes de Customer Success: el Customer Success Specialist, que son perfiles técnicos, específicamente dedicados a facilitar la adopción de cada tecnología; y los Customer Success Managers que son quienes ayudan al cliente a llegar a terminar su Lifecycle, dentro de la arquitectura de tecnologías que tenemos. Y por último, pero no el último lugar, el equipo de Partners, que están dedicados al desarrollo de nuestros socios de negocios para ayudarles a que tengan esa práctica también. Cada uno tiene un currículum muy específico de entrenamiento.

Por último, y en el contexto de "usuarios infieles" en que vivimos, me imagino que la cultura de la organización también tuvo que adaptarse a esta nueva modalidad, a esta nueva visión, a mirar al cliente y monitorear el ciclo completo de vida de su experiencia con Cisco.

Sí, creo que esto es sumamente importante, y aquí regresamos al punto inicial: *"we are in the people's business"*. Y esto tiene que ver con la colaboración, la comunicación, los objetivos en común, una nueva visión compartida. Yo creo que estamos en un proceso cultural muy importante en la compañía, que ya no podemos ser silos, sino que el éxito debe ser común a todos. Y, afortunadamente, creo que en Latinoamérica, tanto Laércio como yo, como los diferentes líderes sabemos que el éxito en común es el único que vale. Hoy tenemos una comunicación abierta, estamos creando diferentes grupos y foros para llegar a ese entendimiento de lo que es la transformación. La transformación no viene por CX, sino que este departamento tiene que ser un vehículo para lograrla, igual que Ventas. Laércio siempre nos recuerda: si no podemos ser los más grandes, podemos ser los primeros, los que estamos incubando y los más admirados. Y hoy tenemos esa oportunidad de crecer en conjunto y lograr resultados bastante buenos con una cultura ganadora, una en la que nos podamos divertir porque estamos haciendo cosas innovadoras. Y tener esa sensación de sentirnos bien alrededor de lo que estamos haciendo. Creo que estamos caminando hacia allá.

Hay una palabra que siempre escucho en las entrevistas que tiene que ver con esto, con sentirse bien con lo que cada uno del equipo hace; y por otro lado, ese sentirse bien, que es honesto, hace que el otro perciba la honestidad.

Sí, la energía positiva se contagia.

Exacto; lo voy a tomar como un aprendizaje. Muchas gracias, Danilo.

Muchas gracias a tí, Karina

Conoce más

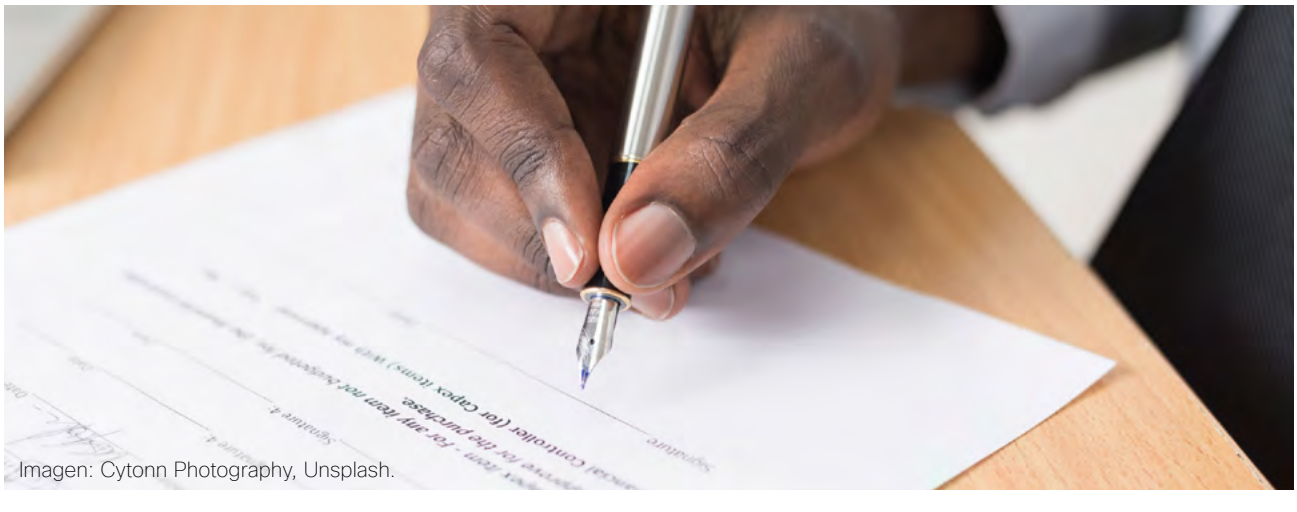


Imagen: Cytonn Photography, Unsplash.

¿Es posible un mundo digital sin contraseñas?

Cada año, entre 20 y 50 % de todas las solicitudes de asistencia técnica de TI son para restablecer contraseñas, según The Gartner Group.

A fin de proporcionar entornos seguros, el método de autenticación sin contraseñas o passwordless es una tendencia que está creciendo en el mundo del trabajo híbrido, en el que los usuarios interactúan con smartphones, PC, laptops, tablets o wearables, y que utiliza datos biométricos, claves de seguridad o un dispositivo móvil.

Con soluciones como Duo Security, se brinda al usuario una verificación a través de múltiples factores y con diversas opciones, que puede ser una notificación al teléfono celular, con un token de hardware o con biometría, buscando liberar a los usuarios de aquellos mecanismos que podrían ser engorrosos o poco habilitadores y también acompañar, por el momento, los repositorios de contraseña, pero que también eventualmente nos vayamos liberando de ellos.

¡Dile adiós a las contraseñas sin comprometer tu seguridad con Duo!

> Click Aquí

Quién es quién

Luz María **Murguía**

por **Karina Basanta**

Nos encontramos con Luz Ma – me permito aquí la abreviación– vía Webex, apenas unos días antes de que dejara su cargo de Latin America Growth Marketing Director en Cisco para dar el salto desafiante al mercado *paytech*. Veintinueve años en la industria de tecnología parecen haber fortalecido a esta líder no solo en sus conocimientos y experiencia, sino también en su afirmación sobre quién es, qué busca y espera de sus equipos, de los entornos y de la vida.

Luz Ma inició en RR.PP., es comunicóloga y está basada en la ciudad de México. Durante casi 20 años estuvo en la empresa Oracle, donde vivió cien por ciento la evolución de una empresa de tecnología a software y luego a la nube.

Hace casi seis años fue invitada a formar parte de Cisco para liderar el equipo de Marketing de México y conformar un conjunto integrado por especialistas en contenidos con foco en satisfacer las necesidades del país. Ya en la gestión, transitó el cambio del contenido creado para tecnologías al actual generado para audiencias. Esta tarea duró casi dos años. A partir de allí fue promovida con el objetivo de liderar el equipo de Latinoamérica. Aquí se afianza la segmentación por audiencias y se suma el segundo idioma: portugués. Sin embargo, lo más destacado de la gestión fue lo que ella denomina la "maestría en marketing y comunicación digital".

"Cuando entré a Cisco yo decía: no hacemos marketing digital, hacemos marketing en un mundo digital. Ambas cuestiones son totalmente diferentes. Hacer marketing digital te limita, hacerlo en un mundo digital te lleva a desarrollar agilidad y un constante aprendizaje, visualización de los datos y optimización de tus tareas, y por ende a buscar la innovación. Ese sí es uno de mis "quotes": hacer marketing en un mundo digital. Nuestro equipo vivió la transición del field marketing al entendimiento de esta nueva tendencia y su nomenclatura: qué es una estrategia de programatic, o de SEM (Search Engine Marketing), o de SEO (Search Engine Optimization) y de qué forma las podemos perfeccionar. Puedo decir que al día de hoy, todos en el equipo de marketing conocemos cómo se optimizan las estrategias a nivel digital y vivo eso como un gran logro. Tuve la fortuna de tener un equipo extraordinario de especialistas en donde cada uno de ellos desde su área hizo su valioso aporte".

Imagen: Bisakha Datta, Unsplash.

El marketing B2B tuvo un gran viraje en estos últimos años, ¿verdad?

El marketing B2B (Business to Business) se conocía como marketing de relaciones, donde teníamos la etiqueta de "eventos". Uno de los objetivos que me propuse fue quitarnos esa etiqueta. Marketing es mucho más que eso: es aportar un conocimiento más profundo del cliente a través de los datos (data insights and analytics) para tomar decisiones basadas en información y no por feeling. Además, estar cerca del negocio nos permite colaborar en acelerarlo, promover nuevos negocios y dar aportes para retener clientes. Es el signo del infinito: no basta con la venta, hay que buscar la recompra, la renovación del software...

¿Cuáles fueron tus principales estrategias en Cisco?

Las grandes estrategias en donde me enfoqué fueron:

- Una comunicación certera de cuál es la necesidad del negocio.
- Cómo marketing puede aportar valor.
- De qué forma marketing puede acercarse más a su cliente interno: Ventas.

En relación a esto, algo muy importante para mí en Cisco fue gestionar las audiencias. Me enfoqué en cuatro:

- La audiencia interna. Puedes gastar millones de dólares en inversión para posicionar tu mensaje, pero si tu vendedor no es consistente en el momento de atender al cliente, definitivamente pierdes toda oportunidad. Para mí, una audiencia inicial fue el empleado, por ello elegimos darles una sobre comunicación sobre las gestiones de nuestro departamento.
- El partner. Nuestro negocio está 97% guiado e influenciado por ellos, por eso el mensaje que emite Cisco debe estar siempre alineado al del partner.
- El cliente final. A esta audiencia la segmentamos luego de la incorporación masiva del trabajo híbrido, entonces nuestro mensaje llega ahora no solo a la persona de tecnología donde nos constituimos como sus mentores y guías, sino también a la de capital humano, la de operaciones, la de logística.
- Los influenciadores. Si bien esta audiencia no reporta directamente a marketing es un grupo de gran importancia. Aquí la alineación se da con la gente de relaciones públicas y analistas.

La migración de vender productos en caja a SaaS hace que el foco se ponga en el contenido y al ubicarse allí también se pueden prever tendencias dentro de los clientes. Marketing puede absorber esas tendencias, que Ventas todavía no está viendo porque está sobre el producto/servicio que tiene disponible para ofrecer. Marketing a través de su lectura de tendencias puede impulsar el desarrollo un nuevo negocio.

Absolutamente de acuerdo. En el momento en que entras en una tendencia de análisis es donde el *Account Base Marketing* ayuda. En Cisco podemos seguir la huella digital del cliente de, por ejemplo, nuestro canal más importante que es cisco.com, tú puedes llegar a un vendedor y decir: "mira el recorrido que hizo este cliente: entró por un podcast, luego se fue a una solicitud de demo, de allí a ver un caso de éxito y terminó en un *click to chat* para pedir más información".

Gracias a la tecnología y a los datos, el marketing B2B se ha convertido en un business *partner* en lugar de un ejecutor y es así como me siento dentro del negocio: me siento como un business *partner* que con base en datos e información define en conjunto la estrategia en la que enfocarnos.

COVID-19: ¿Cómo reaccionó tu área?

Cisco, contaba con el gran beneficio de tener el *home office* y la tecnología disponible. Todos teníamos una gran incertidumbre, sin embargo sabíamos que era importante compartir lo que estaba pasando tanto al cliente interno como externo.

Webex y Seguridad fueron los dos productos que nos activaron a comunicar fuerte tanto en español como en inglés. Estas dos líneas se convirtieron en la punta de lanza en cuestión de activación de contenido, de datos, de referencias. Los casos de éxito me han marcado, siento que Cisco es otro desde que yo entré: me gusta escuchar a Cisco como un influenciador, pero prefiero escuchar la voz del cliente, pues su impacto es mayor.

Imagino que no habrá sido fácil comunicarse con todas las audiencias de forma digital... ¿cuáles fueron los principales retos?

Cierto que hubo retos. El principal fue la fatiga digital. Para ajustarnos a ella hicimos dos grandes cosas:

- La primera fue dar la oportunidad al cliente de decidir cuándo quiere escucharnos o participar de nuestros eventos. A partir de allí, disponibilizamos el material en nuestra plataforma de contenidos *on demand*. Tengamos en cuenta que toda la actualización de contenido fue muy importante porque había que alinearse al contexto que trajo la pandemia.

- La segunda fue la incorporación de los *Podcast* para que el usuario pueda escuchar temas que le interesen mientras realiza otra actividad, como caminar, por ejemplo.

A tu entender, ¿cómo se produce la innovación?

El constante cambio nos empuja a adaptarnos y crear nuevas opciones de innovación, y la innovación se genera gracias a la visualización del comportamiento del cliente. Sabes que algo está en decadencia cuando accedes a la información que devuelve el usuario y la analizas (precisamente las mediciones sobre cada acción realizada: *open ratio e-mail, downloads*, etc.). Saber cómo eran recibidas nuestras acciones de marketing en Cisco nos permitió innovar, por eso llevamos adelante los podcast, los eventos a demanda y la interacción virtual. Nuestra nueva propuesta son las *Masterclass*, de las cuales la primera será sobre Hybrid Work. En este sentido, también hemos encarado un cambio en la forma de exponer la información en el sitio web de Cisco para priorizar la venta.

Además, creo fuertemente en la generación de comunidades que relacionen clientes con afinidades en común, como por ejemplo algunas que llevamos adelante en Cisco: *Running Club, Meet & expert y Meet executive*.

> *“Si está funcionando, replícalo. Si no está funcionando, deja de hacerlo.”*

Social selling y Social Influencing ¿cómo se abordan en Cisco?

Durante la pandemia nos dimos cuenta que si bien teníamos un crecimiento exponencial en la redes sociales tanto en español como en portugués, nuestros empleados son una gran fuente de información e influencia, entonces empezamos a trabajar bajo un programa llamado *Digital Believer*. Se trata de un programa interno que se extendió a los *partners*. Buscaba concientizar primero al empleado sobre la relevancia que tienen las redes sociales, qué objetivo

Imagen: Gentileza Luz María Murguía

> *“El equipo es quien hace que las cosas sucedan.”*

tiene cada una y cuáles son sus diferencias, y al mismo tiempo invitarlos a publicar el contenido que cada quien quiera publicar. Se trata de tomar conciencia de cómo el social *influencing* de los integrantes de Cisco es importante.

Para ello trajimos expertos que hablaron de marca, de *storytelling*, de la importancia de las redes sociales. Además, acabamos de terminar una estrategia llamada “*Digital Adopción Academy*” que inició hace casi tres años y que buscaba repasar las distintas formas de crear contenidos digitales: de qué forma hacer una e-mail, un post de LinkedIn, cómo te conviertes en un influenciador... incluyendo lo básico de cómo está conformado tu perfil y qué confianza vas a generar con él. En Cisco ya estábamos preparados para abordar temáticas digitales antes de la pandemia tanto desde la tecnología que utilizábamos como de la comunicación interna y hacia el cliente.

En tu experiencia, ¿cuáles son las principales redes sociales para hacer mkt. B2B?

Creo que hoy las principales son LinkedIn, Twitter e Instagram. Ahora se sumó TikTok con mucha fuerza e *influencers* con gran cantidad de seguidores y repercusión.

A su vez, el éxito se ve potenciado ya que hoy cualquier integrante de la organización puede compartir las piezas generadas en redes sociales, sobrecomunicar y a la vez, escuchar la voz del cliente. Una campaña con fuerte intervención de los empleados que tuvo mucha repercusión en Cisco fue la que llevamos adelante durante la semana de la ciberseguridad.

Por otro lado, un formato que nos está empujando es el video marketing. A mí me dan mucho resultado los videos espontáneos que me muestren tal como soy, auténtica. Parte de nuestro *Digital Believer Academy* en Q4 va a incluir la estrategia de cómo hacer videos de alto impacto.

¿Cómo defines tu tipo de liderazgo?

Me considero una líder por influencia y no por jerarquía. A veces es necesario hacer el quiebre de la frontera de reporte, porque el gran valor es tener una estructura que trabaje en conjunto y orquestadamente en pos de un objetivo claro, sin importar a quién se reporte.

"Respeto.
Relaciones.
Resultados.
Reconocimiento.
Resiliencia."

Las 5 R de Luz Ma

Cisco es una empresa comprometida con la diversidad y la inclusión, tú una mujer con casi treinta años en el mundo de la tecnología, parece que la fantasía de Cisco y la tuya son compatibles.

Dentro de la cultura Cisco, Diversidad e Inclusión son dos temas de gran importancia. En los últimos dos años fui co-líder de la Comunidad de Woman of Cisco LATAM y parte del Board Member del Woman of Cisco Americas, eso me permitió colaborar con la estructura más allá de mis tareas tradicionales. Hoy soy miembro del 30% -Club.

Estás haciendo un cambio importante al pasar al mercado *paytech*. Cuál es tu última reflexión en esta entrevista con respecto al equipo de marketing de Cisco.

Es cierto, creo que es un buen momento para seguir aprendiendo y construyendo mi crecimiento profesional con un nuevo desafío. Como reflexión te diré que hoy el marketing está mucho más atado a la valoración del negocio que a una ejecución aislada. Orgullosamente dejo a un equipo extremadamente preparado con valores muy sembrados de trabajar en conjunto, de comunicar y sobrecomunicar, de enfocarse en la voz del cliente, de adoptar la digitalización... he sido su líder estos últimos tres años, aquella que ha tenido el privilegio de guiarlo hacia adelante y estoy agradecida de su aceptación y compañía

#Teamwork Makes the dream work #constantLearning

Nunca hay una segunda oportunidad para dar una primera buena impresión

Sellos de Luz Ma

Siempre he comentado a mis equipos que tener estrellas fugaces no me funciona. Brillar por sí mismo, no me funciona. ***Lo que busco es tener una constelación donde todas las estrellas brillen en conjunto con un mismo objetivo.*** Creo que ese es uno de los grandes valores de mi equipo en Cisco: todos suman y la prioridad es estar cerca para dar respuestas al negocio.

Lado B

“Cuando conecto con las personas, difícilmente desconecto de ellas.”

Soy la séptima de ocho hermanos. Creo que el primer *teamwork makes the dream work*, es decir el primer círculo de respeto y de admiración fue mi familia. Yo soy la chiquita y la primera generación femenina que tiene una carrera universitaria… luego ya tenemos ingenieras, doctoras, en breve mi hija empieza la carrera de ingeniería biomédica. Sin quererlo e ido impactando a las siguientes generaciones con el modelo del estudio y el crecimiento profesional.

Soy una persona:
espiritual.

De no haber sido marketera hubiera sido:
Psicóloga.

Por qué:
para escuchar a la gente.

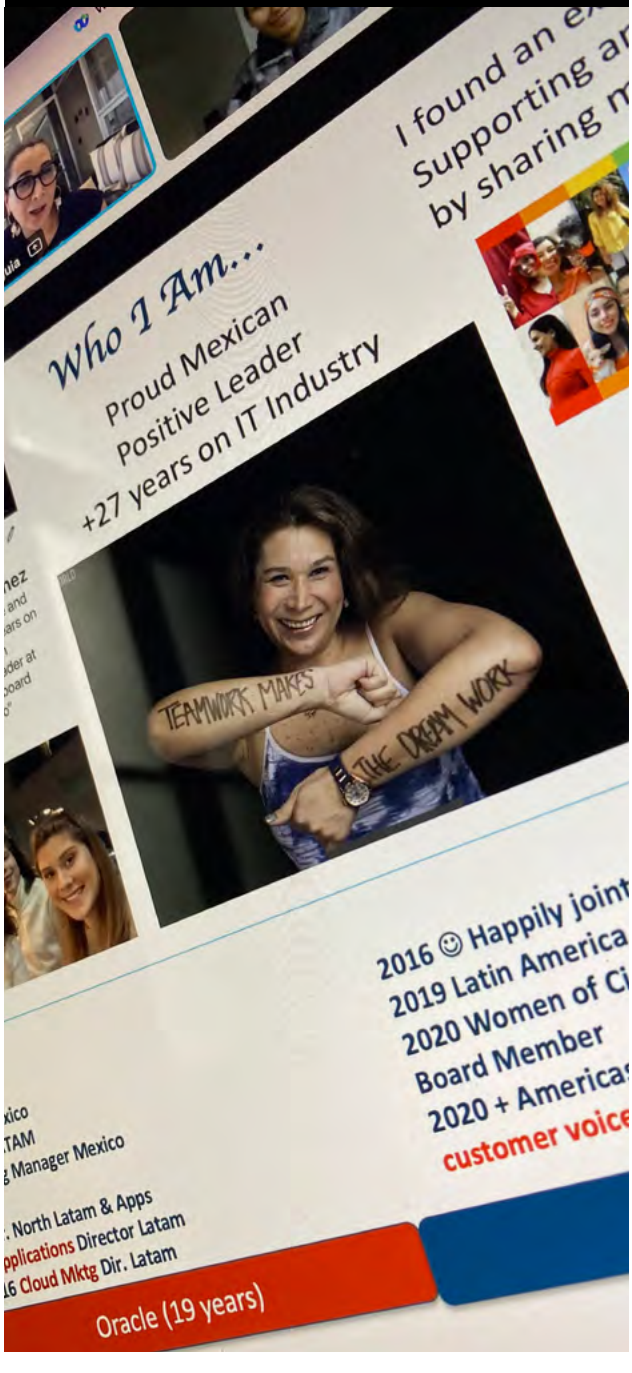
Tu don:
ayudar a las personas.

Cuando te retires:
cuando pueda ser Board Member me gustaría viajar e ir por la India a presenciar lo que es el beneficio de la meditación.

En qué confías:
en la energía y en los ángeles.

Un amor:
los elefantes.

Por qué:
porque tienen orejas grandes para escuchar mejor.



Instagram de LuzMa
@luzma_positiveimpact

De la editora:
La escucha define a Luz Ma, busca el dato para concretarla.

Dionisio o Damocles: esa es la cuestión

El Rey Dionisio "El viejo" fue un sanguinario tirano que vivió en Siracusa alrededor del siglo IV a.C. En su corte había varios aduladores, como era habitual, pero entre ellos se destacaba uno, Damocles, quien se la pasaba envidiando los lujos y comodidades del tirano. Un día, Damocles, corroído por la envidia, habló con Dionisio y le dijo: "¡Debes estar muy feliz! Tienes todo lo que un hombre puede desear: fama, dinero, admiradores…". El Rey cansado de las adulaciones envidiosas planeó un escarmiento para Damocles, le propuso un intercambio de roles para que pudiera disfrutar de los placeres de ser Rey por un día, Damocles aceptó inmediatamente sin pensarlo y el Rey encargó un banquete para esa misma noche. Cuando se encontraba sentado en la silla del Rey, disfrutando de los exquisitos beneficios, se percató que sobre su cabeza pendía una espada atada a un fino pelo de crin de caballo. En ese momento olvidó los privilegios y solo le preocupaba morir en cualquier momento. El Rey le preguntó qué sucedía y cuando Damocles le señaló la espada, Dionisio le respondió: "Sé que hay una espada amenazando tu vida, sin embargo ¿por qué debería preocuparte? Yo estoy siempre expuesto a peligros que podrían hacerme perder la vida en cualquier momento." Inmediatamente Damocles rogó intercambiar el puesto y abandonar todos los privilegios y beneficios que este traía.

No es claro si este hecho sucedió o fue un invento del filósofo Cicerón para mostrar realidades y exponer los fundamentos de la felicidad, pero esta historia es muchas veces utilizada para mostrar lo poco evidente que puede ser la responsabilidad y el peso de una posición o trabajo. También representa una situación que era poco evidente y significativa hace un par de años.

Los aventurados

Previo al inicio de la pandemia, las áreas de seguridad, dirigidas por los más aventurados en la materia, eran equipos de trabajo supeditadas a la gerencia de Tecnología o al área de Gobierno, Riesgo y Cumplimento. Estas áreas estaban conformadas por pocas personas que entre muchas labores debían repartir su tarea en la definición y auditoría de políticas de seguridad para el correcto cumplimiento de alguna norma o regulación a la que la compañía estuviera obligada, y subrayo, obligada estrictamente a cumplir.

En general, cuando eran convocados a participar en los proyectos se los incluía en las reuniones sobre el tramo final del proceso, previo a una salida a producción, con el único objetivo de dar el visto bueno a una herramienta que llevaba siendo implementada por un equipo de ingenieros durante los últimos 12 meses o más.

Claro que todos en esa mesa esperaban una aprobación rápida al proyecto, y claro que eso no sucedía porque era en ese momento cuando eran advertidos de todos los riesgos, vulnerabilidades y principios de arquitectura de seguridad que habían sido omitidos. Cuando esto pasaba, las reuniones terminaban mal, con la mitad de la mesa señalando al área de seguridad como un contradictor al progreso del proyecto, un *stopper* que no entendía la urgencia del negocio y la estrategia corporativa, que se había quedado estancado en sus políticas y sus extra controles, en su cueva de ermitaño sin entender la realidad empresaria.

Y llegó la pandemia

En este contexto llegó el 2020 y un virus proveniente de China comenzó a cambiar la realidad del mundo. Como en una ficción se empezó a hablar de cuarentenas y aislamiento de ciudades enteras en ese país. No fue hasta que nos tocó de cerca que nos dimos cuenta de la seriedad del tema. Nos aislamos y seguimos nuestras vidas, pero ahora conectados desde nuestras casas, asistiendo a nuestros hijos para que pudieran iniciar sus clases por videollamada, mezclando la computadora personal con la laboral y las Webex familiares con las laborales.

En ese contexto, todos los ojos se volcaron sobre el área de seguridad. De alguna forma era necesario flexibilizar las medidas y controles que durante años se habían establecido para las oficinas y data centers con el fin de permitir que todos pudieran conectarse desde su casa a aplicaciones, servidores y bases de datos que por años estuvieron kilómetros adentro de

Ad Content

por **Fabio Sánchez**

Director práctica de Ciberseguridad,
OCP Tech.

Imagen: Ricardo Cruz, Unsplash.

la zona desmilitarizada, protegidos por 2 o más *firewalls* y con accesos restringidos; de un momento a otro estos equipos estaban nuevamente en el ojo del huracán, debían actuar rápido y entender la nueva estrategia corporativa y urgencia de negocio. Así lo hicieron… todo se hizo para que el negocio siguiera funcionando.

El peso de la espada

Pero en ese momento la espada que se balanceaba sobre sus cabezas se hizo más pesada y el fino pelo de crin de caballo, más débil. Pocos entendieron la dimensión de los riesgos que se asumían y el nivel de exposición a la que las empresas quedaron expuestas desde el inicio de la pandemia, al punto que recién ahora se están viendo las consecuencias de años de presupuestos recortados y limitación del personal de seguridad.

De acuerdo al reporte sobre Cibercrimen de Interpol [1] las principales amenazas por la pandemia de COVID-19 en 2020 fueron *Phishing/Scam* con 59% y *Malware* y *Ransomware* con un 36%. Esto obedece a que la superficie de ataque aumentó como fruto del cambio hacia el teletrabajo, estilo al que las organizaciones tuvieron que rápidamente adaptar sistemas para acceso remoto, infraestructura y aplicaciones que antes eran solo accedidas desde las oficinas centrales y sucursales. El mismo informe menciona que en abril de 2020 se dio un pico de ataques de *ransomware* por múltiples grupos ciberdelincuentes que meses atrás se encontraban inactivos, acción que implícitamente podría indicar que existe *ramsomware* desplegado pero aún no activo esperando ser utilizado en momentos específicos para maximizar su impacto y precio por el rescate.

Después de dos años el panorama en las compañías sigue muy similar, muchas compañías no cambiaron y volvieron a la realidad de la prepandemia, incluso algunas todavía afirman que el trabajo de las áreas de ciberseguridad no es tan complejo y no requiere mayor inversión de personal y recursos tecnológicos, que solo deberían ceñirse a definir políticas y auditar controles que manualmente sean viables sin entorpecer los procesos de negocio. Nada está más alejado de la realidad y cada día el riesgo aumenta.

Hacia un nuevo paradigma

Urge entonces un cambio de paradigma. Un estudio realizado por Gartner pronostica que para el 2023 el 30% de los CISOs (Chief Information Security Officer) no solo deberán cumplir y ser responsables de la ciberseguridad de la compañía sino que además serán medidos directamente por su habilidad de aportar valor al negocio [2]. A primera vista esto parece contradictorio y muestra un futuro aún más incierto para las áreas de seguridad:¿cómo se puede ser más activo y seguir la velocidad que los negocios requieren y al mismo tiempo aportarle valor?

Para generar valor al negocio, la teoría general menciona que existen 3 factores a considerar: la imagen pública de la empresa, la percepción que los consumidores tienen de la misma y la efectividad de sus productos y servicios. Desde las áreas de ciberseguridad existen muchas formas en las que debemos generar valor y desde la mano de los ingenieros expertos de OCP TECH hemos desarrollado proyectos que garanticen y aporten valor a las compañías.

Cuando una brecha de seguridad es expuesta por atacantes filtrando datos privados de clientes, no hay nada que se afecte más que la imagen de la empresa, que tendrá que responder directamente ante autoridades judiciales y clientes por la información robada.

Todas las medidas que se tomen para la prevención de estos hechos ya sea mitigando riesgos conocidos como concientizando a los empleados de las organizaciones sobre los ataques a los que están expuestos, genera y preserva el valor de las compañías a largo plazo. Debemos entonces ser más asertivos en la forma de presentar los proyectos, justificar los casos de negocio y el costo total de propiedad de soluciones y proyectos de seguridad, pues ya no nos podemos limitar a mostrar el ahorro de costos que una herramienta puede brindar o regulación y norma que la justifica, debemos ir más lejos y facilitar la alineación a mediano y largo plazo con la estrategia de la compañía.

La mirada del consumidor

Por muchos años el consumidor se limitaba a ver los beneficios que le daba el producto y/o servicio y su costo comparado con productos similares o sustitutos, siempre guiado por su intuición. Esto ha evolucionado y es cada vez más complejo entender la mente de los usuarios. Hoy en día seleccionan un producto influenciados por una celebridad o por un video que vieron millones de personas en internet, pero si algo puede realmente influenciar en la compra de un producto o servicio es la percepción de confianza que este representa. Cuando estamos adquiriendo un servicio esa percepción puede verse afectada si una empresa no se toma en serio los riesgos de seguridad a los que están expuestos los clientes.

Métodos de autenticación, esquemas de prevención de fraude y factores de autenticación biométricos ya no son vistos por los usuarios como un dolor de cabeza y un impedimento en el uso de los servicios, sino que se perciben como elementos que los aseguran a ellos y a sus compras. En OCP TECH tenemos soluciones enfocadas en gestión de accesos de clientes, con métodos de autenticación fuertes y autenticación biométrica que se adaptan a las herramientas y soluciones digitales que las empresas ya posean sin deteriorar la experiencia de cliente en los diferentes canales digitales

[1] COVID-19 Cybercrime Analysis Report- August 2020 - INTERPOL General Secretariat 200, quai Charles de Gaulle, 69006 Lyon, France.

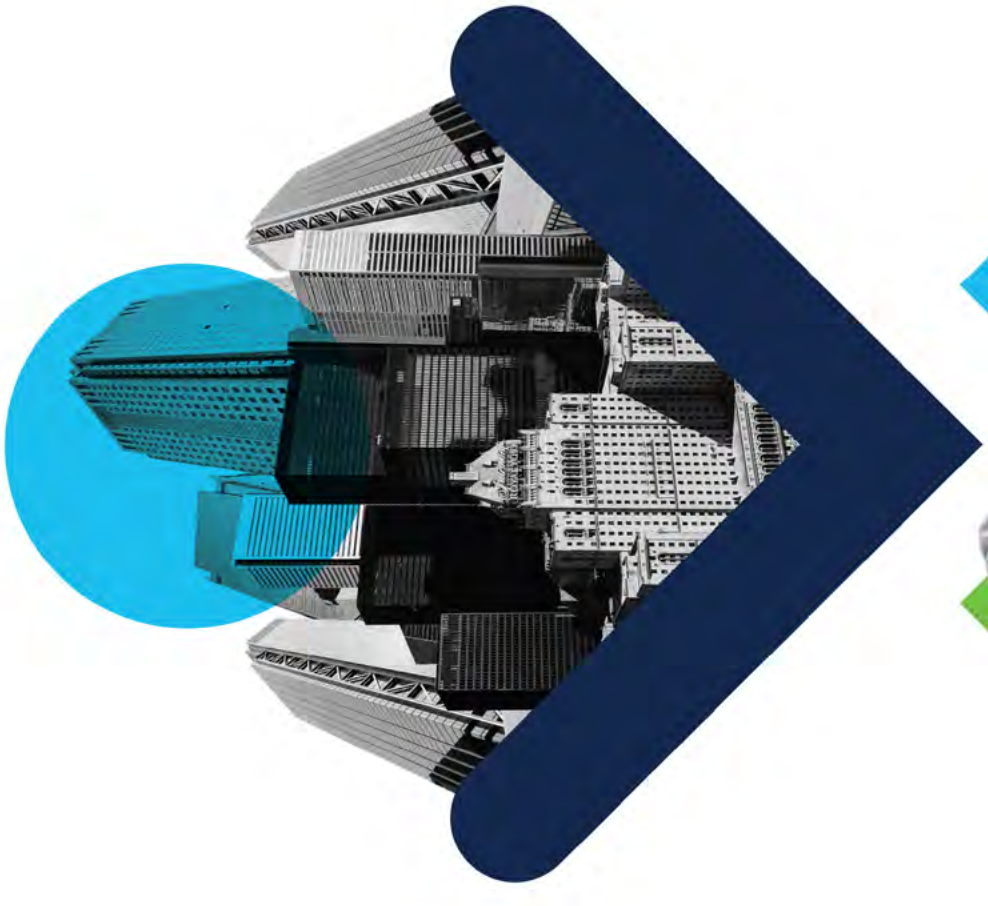
[2] Rethink the Security & Risk Strategy - Embrace modern cybersecurity practices while enabling digital business. EDITED BY Tom Scholtz Distinguished VP Analyst, Gartner

CISCO
SECURE X

Experiencia simplificada

La plataforma Cisco SecureX es una experiencia integrada dentro de nuestra cartera de seguridad que se conecta con toda su infraestructura de seguridad.

Conozca más



CISCO The bridge to possible

Columna

Smart Supply chain

“Ciberseguridad basada en los habilitadores Blockchain, ZKP y Zero Trust

Contenido audiovisual

Imagen: Ryutaro Uozum, Unsplash.

por **Freddy Macho**

Presidente del Comité IoT de la Comisión Expertos
Laboratorio Ciberseguridad OEA
Presidente Centro de Investigación de
Ciberseguridad IoT – IIoT
Coordinador del Centro de
Ciberseguridad Industrial (CCI)
Chairman IoT Security Institute LATAM

La transformación digital ha abierto una nueva forma de vivir y trabajar. A medida que el rendimiento y los nuevos niveles de conectividad permiten a las empresas aprovechar los beneficios de las tecnologías innovadoras, el mundo se vuelve más rápido, más flexible y más eficiente. Este cambio está creando un ecosistema global donde las cosas físicas y digitales están cada vez más conectadas, desde activos de infraestructura críticos hasta personas y datos.

Por esta razón las empresas deben invertir tiempo y recursos en revaluar sus cadenas de suministro para encontrar y abordar las debilidades. La cadena de suministro fue el sector que más ataques sufrió a raíz de la aparición de la pandemia a nivel global en el 2020.

Antecedentes

A medida que avanzamos hacia un mundo más globalizado y cada vez más complejo en su dependencia de los componentes de software, el riesgo de la cadena de suministro ha evolucionado y se ha expandido. Si bien los problemas de este tipo en sectores como el energético se han reconocido y estudiado durante varios años, aún persisten.

La Corporación de Confiabilidad Eléctrica de América del Norte (NERC) está actualizando sus estándares de Protección de Infraestructura Crítica (CIP) para incluir protecciones de la cadena de suministro, sin embargo existen brechas: NERC-CIP se aplica solo a un subconjunto de sistemas y componentes que afectan la seguridad y la confiabilidad en un subconjunto de servicios eléctricos, y medir la seguridad de Internet es, en el mejor de los casos, un indicador indirecto de la tecnología utilizada en sistemas de control.

En diciembre de 2015, cientos de miles de hogares ucranianos quedaron temporalmente a oscuras en el primer ciberataque confirmado contra una red eléctrica. En agosto de 2017, las contraseñas predeterminadas codificadas (una clase conocida de vulnerabilidades de la cadena de suministro) en un componente de sistemas instrumentados de seguridad facilitaron el cierre de las operaciones de Saudi Aramco, siendo objeto así de un nuevo ataque después del sufrido el 2012.

En diciembre de 2020, una empresa de ciberseguridad descubrió una campaña global de intrusión cibernética que comprometió primero el código fuente y luego actualizó la plataforma Orion de SolarWinds, un producto de software de administración de TI ampliamente implementado. La actualización corrupta fue descargada por miles de clientes de SolarWinds y abarcó agencias gubernamentales de EE. UU., entidades de infraestructura crítica y organizaciones del sector privado. Este ciberataque puede no tener precedentes en escala y sofisticación y es consistente con una serie de tendencias persistentes en el uso de vectores de la cadena de suministro.

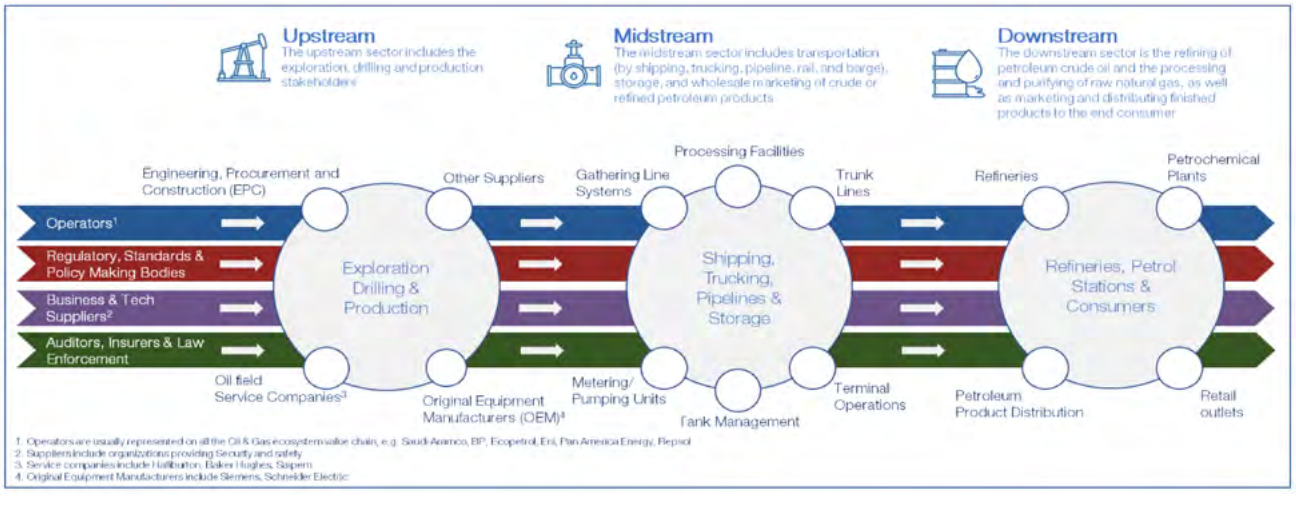
Durante el fin de semana festivo del 4 de julio del 2021 en EE. UU., una banda criminal explotó una vulnerabilidad del popular software de gestión de TI, Keseya VSA, utilizado por más de 36.000 clientes en todo el mundo, para perpetrar uno de los mayores ataques de ransomware en la cadena de suministro de la historia.

Imagen: Software Supply Chain Attacks – ASSESSMENT OF THE CRITICAL SUPPLY CHAINS SUPPORTING THE U.S.

Gestión de riesgos de terceros en la cadena de suministros

Los ataques a la cadena de suministro han tenido consecuencias operativas, financieras y reputacionales dramáticas. Estos eventos no solo afectan a la víctima, sino a todas las partes interesadas en la cadena de valor y demuestran la importancia de adoptar un enfoque colaborativo y holístico al gestionar los riesgos de terceros.

Las empresas pueden tener requisitos divergentes debido a la singularidad y complejidad del modelo de negocio. En la industria del petróleo y el gas, por ejemplo, la digitalización vertiginosa de las empresas de fabricación aumenta la complejidad de controlar el riesgo derivado de terceros dentro de su cadena de suministro. La mayoría de los enfoques de gestión de riesgos de terceros dependen de la configuración interna, la cultura y las prioridades de la organización. Los procesos y requisitos actuales en la industria siguen siendo conservadores.



Riesgos de terceros en la industria del petróleo y el gas - Cyber Resilience Oil and Gas of World Economic Forum's.

La cadena de suministro se ve apoyada en todos los sectores por un número representativo de pequeñas y medianas empresas las cuales ejecutan un presupuesto operativo bajo, que en su mayoría no invierte adecuadamente en ciberseguridad. Por lo tanto, se están convirtiendo en los objetivos preferidos de los ciberdelincuentes, ya sea como objetivos directos o como vector de ataque para llegar a las empresas más grandes, las agencias gubernamentales o las infraestructuras críticas a las que suministran servicios.

Durante una investigación realizada por la Dirección Nacional de Cibernética de Israel (INCD), muchas pymes se quejaron de los requisitos demasiado diversos de los diferentes clientes y reguladores. Las grandes empresas invierten una gran cantidad de recursos en la definición de sus propias necesidades para la gestión del riesgo cibernético de acuerdo con estándares como ISO 27036, 800-161 y otros, sin embargo, a menudo se conforman con las declaraciones de los proveedores en lugar de insistir en resultados de auditoría válidos.

Reconociendo el riesgo en todos los ámbitos, el Centro Nacional de Seguridad Cibernética (NCSC) del Reino Unido publicó una guía de seguridad de la cadena de suministro para que las empresas tengan un mayor control de la ciberseguridad. Las pautas son bastante completas y educan a las empresas sobre cómo deben comprender y gestionar el riesgo que se origina en los proveedores, pero gran parte del trabajo requerido se deja a las propias empresas. Una auditoría reciente de INCD, muestra cuántos de los controles de seguridad cibernética individuales de la organización cumplieron con los estándares requeridos.

Existen diferentes enfoques para lograr una ciberseguridad más sólida, principalmente mediante la certificación de productos y servicios. Para que el proceso sea completo necesitamos mejorar el nivel general de higiene cibernética de los proveedores y no solo sus productos específicos.

Garantizar que los productos comprados a través de la cadena de suministro estén certificados y sean ciberseguros es, por supuesto, una capa importante. Sin embargo, la certificación del producto puede ser relevante para una versión específica y puede perder relevancia en la siguiente. Es imperativo complementar el esquema de seguridad con un esquema de certificación de proveedores desde el punto de vista del cliente. Las empresas deben garantizarse de que los proveedores en los que confían mantengan un nivel predeterminado de cibernética que reduzca significativamente los riesgos.

Visibilidad, pilar de la ciberseguridad

Las transformaciones tecnológicas críticas en las que se basa la prosperidad futura (conectividad ubicua, inteligencia artificial, computación cuántica y enfoques de próxima generación para la gestión de acceso e identidad) serán también desafíos para la comunidad de la ciberseguridad ya que estas transformaciones tienen el potencial de generar riesgos nuevos y sistémicos para el ecosistema global. Dos tendencias técnicas resaltan el problema:

Aumento del uso de dispositivos perimetrales/IoT:
piense en el escenario en el que un sensor de temperatura de IoT habilitado para conexión inalámbrica de $5 y una plataforma de gestión logística portuaria de más de $500.000 están en la misma red de comunicaciones. Estos no vienen con la misma inversión en ciberseguridad, como código confiable, parches de seguridad y uso de credenciales seguras. Como tal, se requerirán herramientas de visibilidad de red inteligentes para ayudar a definir la segmentación, agrupar cosas que deberían comunicarse entre sí y aplicar controles de seguridad alineados con los riesgos de estos dispositivos reunidos.

Datos:
conectar cosas permite nuevas posibilidades y oportunidades comerciales ilimitadas. Sin embargo, las leyes de privacidad como GDPR y CCPA a menudo requieren que la información personal solo se pueda compartir dentro de ciertas estipulaciones, como el consentimiento y el propósito. Para compartir datos personales legalmente dentro de estos contextos, será necesario saber qué cosas en su red están recopilando datos personales y definir controles de intercambio aceptables, lo que significa comprender las cosas y el tráfico que les permite comunicarse.

Cuando se trata de visibilidad de datos, las cadenas de suministro son críticas y cada vez más complejas. Esto a su vez requerirá una cadena de infraestructura; tanto en el software en todas las cosas conectadas, el hardware que cada uno usa, los servicios de comunicaciones a través de los cuales se conectan y el hardware de comunicaciones sobre el cual se ejecutan las comunicaciones.

Crear visibilidad en un mundo conectado

En el dominio digital, la visibilidad es clave para habilitar nuevas capacidades. En cualquier proceso digitalizado, necesita tres pilares: (1) Datos que son procesados (2) una "cosa", por ejemplo, un sistema IoT (dispositivo de borde); y (3) conectividad. Efectivamente, la ciberseguridad busca patrones de comportamiento esperados ("normas") para tomar decisiones. Pero a medida que hacemos más conexiones con más cosas nuevas, este alcance se vuelve extremadamente complejo.

Para generar visibilidad, la comunidad de seguridad debe priorizar tres desafíos:

Los estándares todavía están inmaduros a nivel mundial, y los dispositivos IoT a menudo usan sus propios lenguajes de comunicación y se comunican de muchas maneras. Algunos dispositivos usan encriptación, lo que ayuda a proteger los datos, pero dificulta aún más la comprensión de la comunicación en curso y la detección de anomalías sospechosas. Como tal, necesita ciberseguridad que pueda identificar todo y definir normas de comportamiento de manera continua.

Ver **todo el flujo de tráfico** para localizar cualquier problema. Un dispositivo o cosa siempre se conecta a su antena más cercana, lo que le da una dirección de red (un identificador). A medida que el dispositivo se mueve esa identidad cambia. Los protocolos aseguran que la comunicación sea fluida con el dispositivo final. Pero a menos que tenga seguridad cibernética moviéndose con el dispositivo, entonces debe tener herramientas de ciberseguridad que puedan volver a correlacionar este tráfico para encontrar el objeto real que está comprometido debido a un ataque cibernético o vulnerable a un ataque futuro. Para administrar el riesgo, debe realizar un seguimiento de los flujos de comunicaciones en movimiento (tanto en 4G como en 5G), comprender qué se comunica con qué y analizar si funciona según lo diseñado o previsto, o si existe una amenaza.

Por último, los controles de seguridad deben conocer **la segmentación del tráfico y los controles** de priorización. La segmentación de red es un enfoque arquitectónico que divide una red en varios segmentos o subredes, cada uno de los cuales actúa como su propia red pequeña; esto permite a los administradores de red controlar el flujo de tráfico (y priorizarlo según sea necesario) entre subredes.

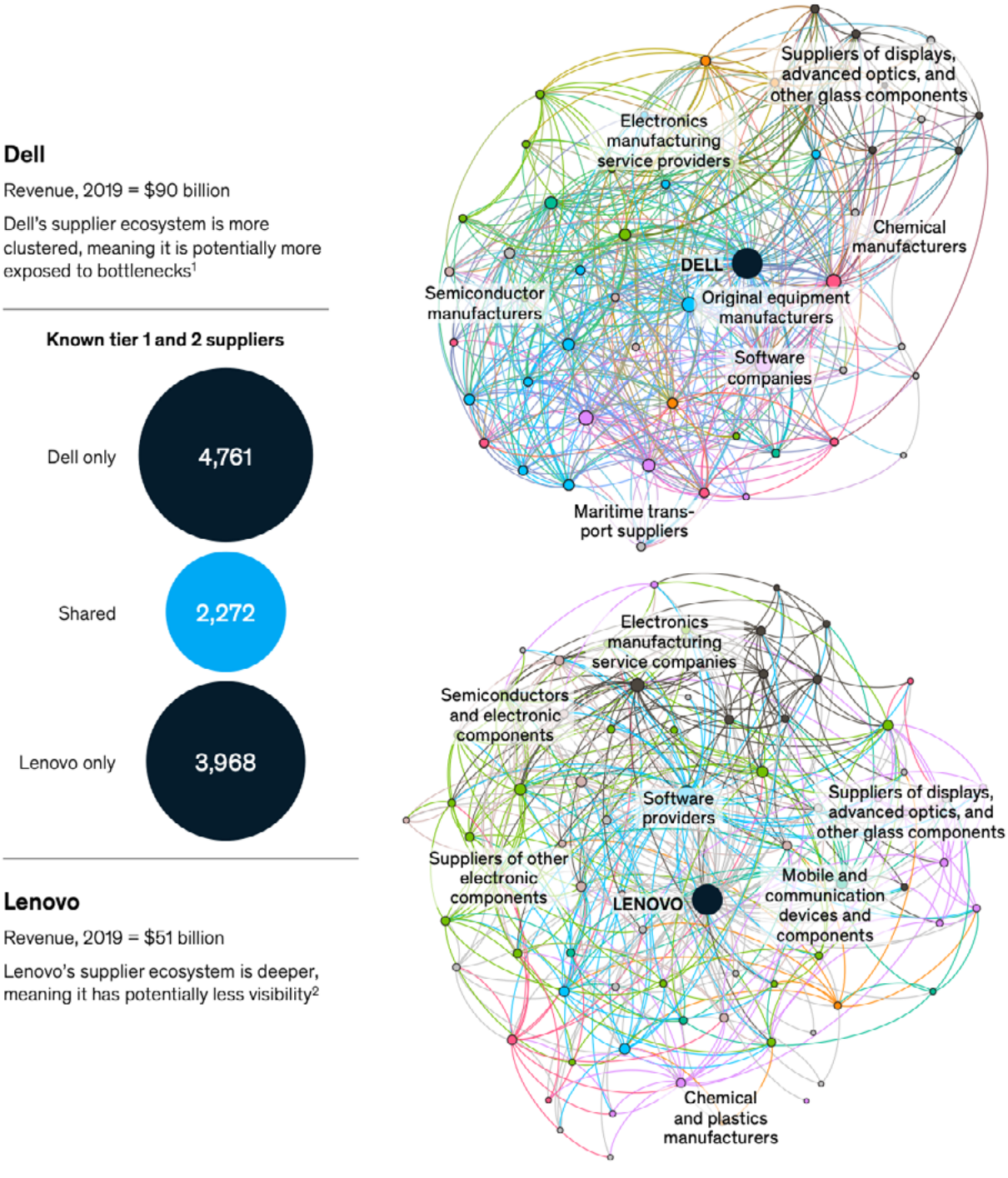


Imagen: ASSESSMENT OF THE CRITICAL SUPPLY CHAINS SUPPORTING THE U.S.

Modernización de la cadena de suministro

Desde la modernización de las cadenas de suministro hasta la priorización de la ciberseguridad, las organizaciones deben actuar para seguir el ritmo de la transformación digital. Una mejor visibilidad de la cadena de suministro puede impulsar los métodos de producción sostenibles y brindar una mayor confianza a las empresas sobre el origen de sus materiales. El sitio de manejo de datos Statista cita una encuesta de 2018 que "encontró que el mayor desafío (21,8%) para los ejecutivos de la cadena de suministro global era la visibilidad".

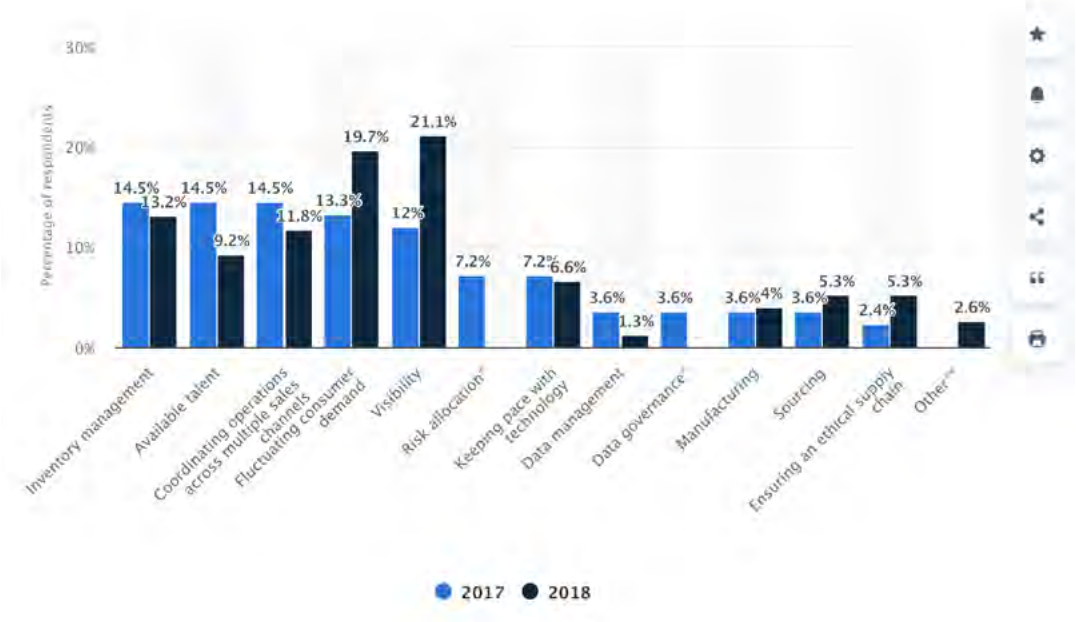
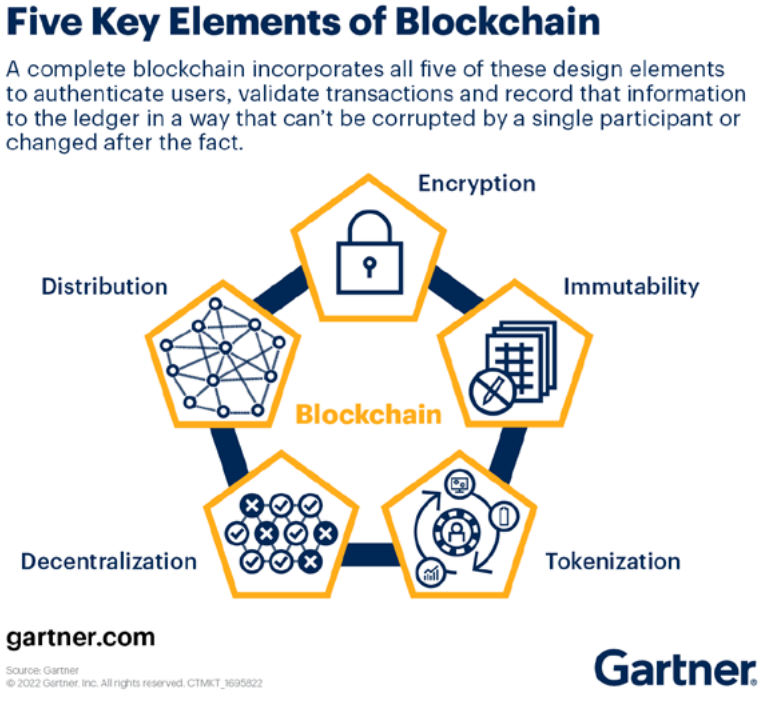


Imagen: Statista -Desafíos de la cadena de suministro.

Blockchain en la cadena de suministro digital

Las cadenas de suministro cada vez más globalizadas y complejas están teniendo un gran impacto en las empresas internacionales. Las partes interesadas dentro de las cadenas de suministro necesitan manejar una mayor cantidad de información mientras realizan el seguimiento de más transacciones, registran el rendimiento y planifican actividades futuras. La logística se está volviendo cada vez más compleja, con más partes involucradas directa o indirectamente en las cadenas de suministro. Esta complejidad está creando desafíos relacionados con la comunicación y la visibilidad de extremo a extremo, lo que hace que los procesos logísticos sean ineficientes.

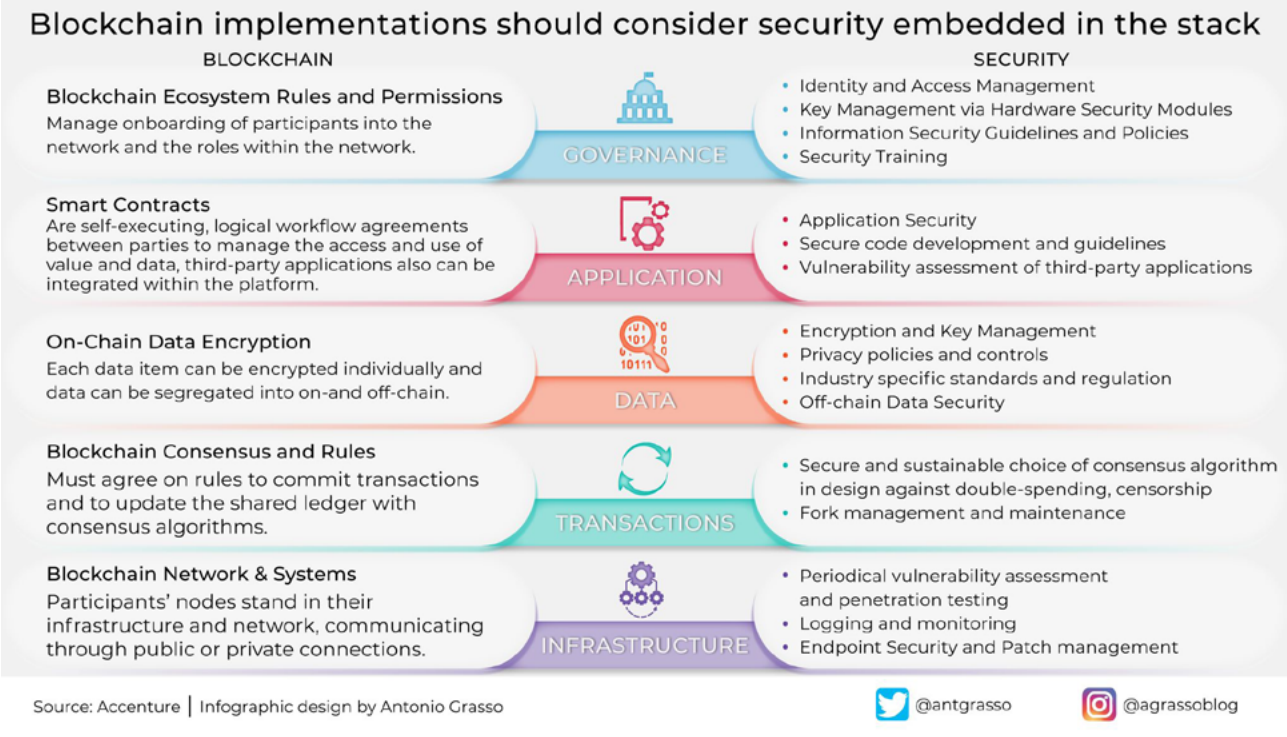
Blockchain es una tecnología basada en Internet que es apreciada por su capacidad para validar, registrar y distribuir públicamente transacciones en libros de contabilidad cifrados e inmutables por medio de una cadena de bloques.



En esencia, una cadena de bloques es una base de datos compartida. Específicamente, el término se refiere a un registro de datos seguro y descentralizado que no se puede cambiar y que se forma a través de una red de igual a igual.

El término "cadena de bloques" se deriva de los "bloques" de transacciones validadas e inmutables y de cómo se vinculan en orden cronológico para formar una cadena (documento). De ahí el término.

En última instancia, blockchain permite que diferentes organizaciones compartan datos de forma segura y logren objetivos comunes de manera más eficiente. Hace posible que las partes interesadas interactúen sin necesidad de una organización de control central. Y puede abrir oportunidades para desarrollar modelos de negocio completamente nuevos.



Beneficios de blockchain en la cadena de suministro

La tecnología puede resolver desafíos claves al crear un registro digital encriptado que rastrea los productos en cada etapa de la cadena de suministro. Hace que cualquier irregularidad que pueda interrumpir un envío sea claramente visible, lo que permite a las empresas resolver los problemas rápidamente. Puede automatizar procesos al mismo tiempo que facilita la verificación de mercancías, reduciendo el papeleo y apoyando la trazabilidad de extremo a extremo.

Mejorar la transparencia y la trazabilidad de la cadena de suministro

- Proporcionar transparencia de extremo a extremo.
- Monitorear el desempeño.
- Confirmar procedencia.
- Aumentar la visibilidad en tiempo real.

Garantizar la seguridad, la inmutabilidad y la autenticidad

- Autenticar datos y documentos.
- Detectar fraude.
- Evitar robos.

Reducir la complejidad del proceso

- Eliminar intermediarios.
- Mejorar la garantía de calidad.
- Aumentar el nivel de automatización.

Mejorar la eficiencia operativa

- Mejorar el cumplimiento.
- Reducir el costo de transacción.
- Reducir el error humano.

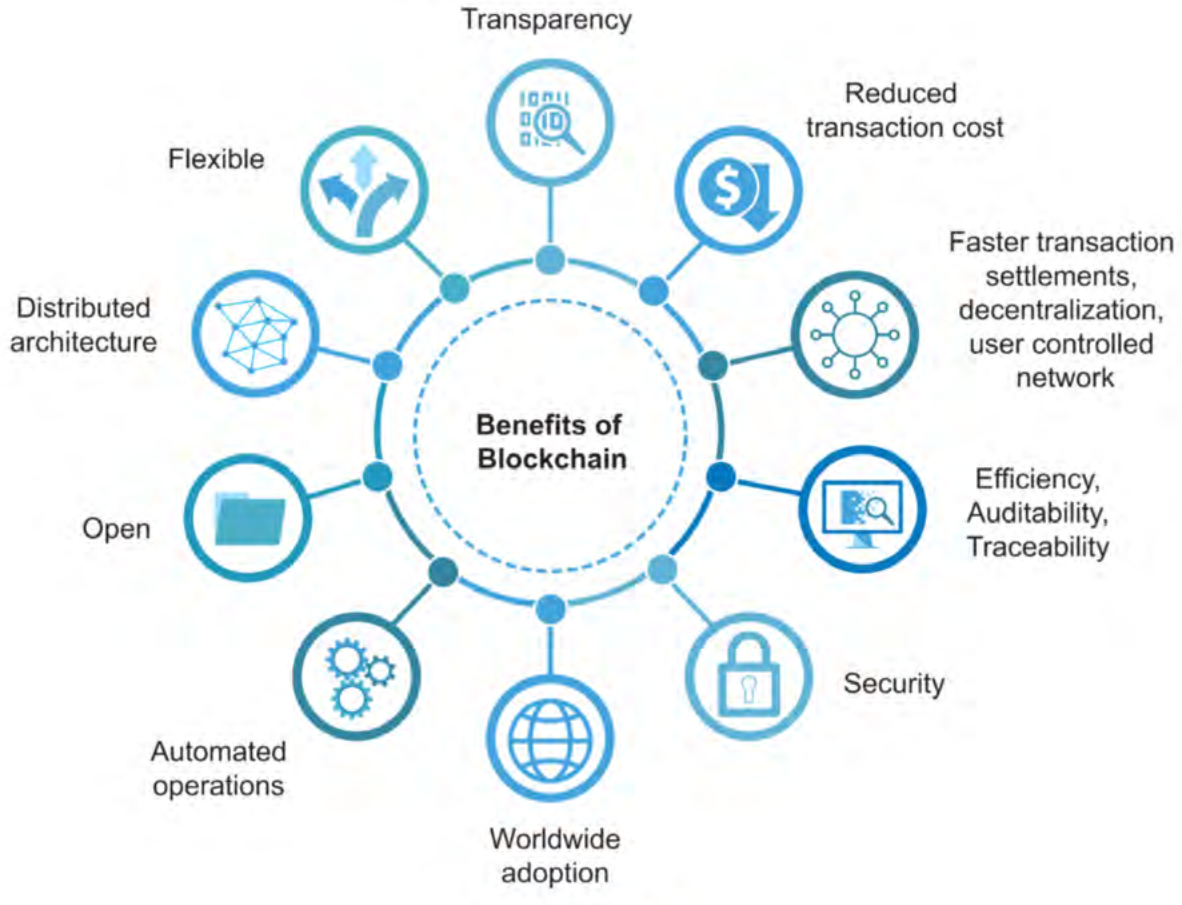


Imagen: Gartner

Casos de uso de Blockchain en logística

Existe un gran potencial para las aplicaciones de blockchain dentro de las funciones logísticas. La tecnología puede resolver desafíos claves al crear un registro digital encriptado que rastrea los productos en cada etapa de la cadena de suministro. Entre los posibles casos en los cuales podrían ser utilizados están:

Procedencia

En logística, la procedencia se refiere a una línea de tiempo de cambios en la propiedad, custodia o ubicación de un objeto. Podría describirse como una pista de auditoría y tiene como objetivo asegurarse de que cada producto enviado tenga un "pasaporte" digital que demuestre su autenticidad. Estos pasaportes incluyen datos sobre dónde y cuándo se fabricó el producto, así como la ruta que ha recorrido.

Pagos y facturación

La facturación y los pagos relacionados con las funciones de logística a menudo implican procesos manuales y en papel porque cada una de las empresas involucradas mantiene registros separados. Hacer coincidir las facturas con los pagos vencidos o acreditados es una tarea que requiere mucho tiempo para las empresas. Blockchain puede almacenar y compartir registros digitalizados, al mismo tiempo que crea contratos inteligentes que manejan automáticamente facturas y pagos para acortar los tiempos de procesamiento y garantizar la precisión.

Documentación digital

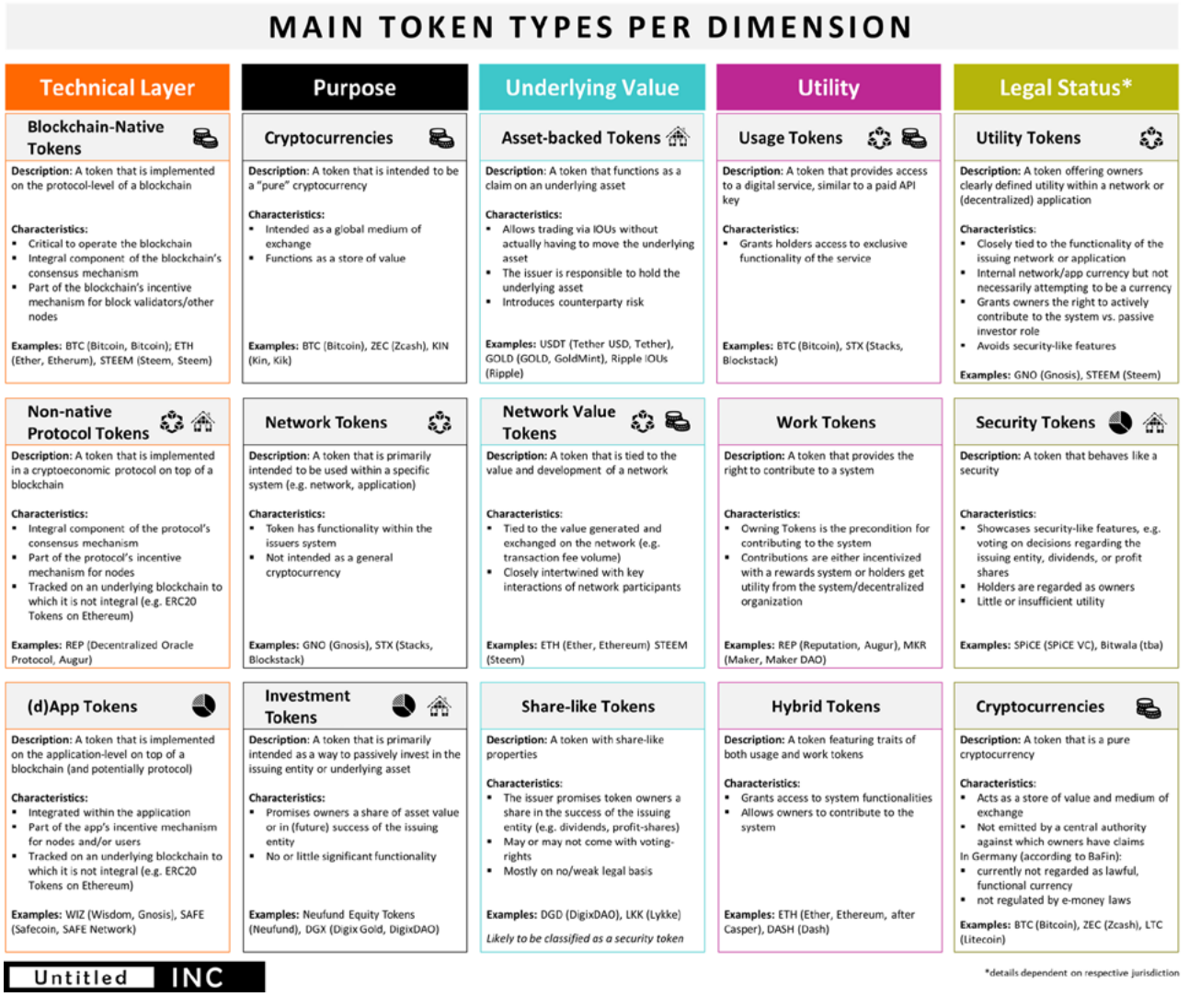
La combinación de blockchain con Internet of Things (IoT) puede permitir contratos de logística inteligentes. Esto es posible cuando los documentos digitalizados (por ejemplo, conocimiento de embarque, certificados, facturas, avisos previos) y los datos de envío en tiempo real estén integrados en sistemas basados en cadenas de bloques. La documentación digital y los contratos inteligentes que utilizan blockchain ya están disponibles en los puertos de Amberes, Róterdam y Singapur.

Gestión de identidad

Blockchain Identity Management es una solución segura que protege las identidades de las personas contra lesiones o robos. Utiliza un modelo de confianza distribuido para garantizar la privacidad donde los participantes autorizados aseguran, verifican y validan los documentos de identidad.

Mercado logístico

Blockchain permite una comunicación fluida e integrada a través de cadenas de suministro complejas. De esta forma, mejora la confianza, la seguridad y la rapidez. Incluso se puede utilizar para crear plataformas donde los proveedores de servicios logísticos ofrecen capacidad gratuita en camiones o barcos en tiempo real.



Zero-Knowledge Proofs (ZKP)
ZKP es un método criptográfico en el que un probador puede convencer a un verificador de que conoce un valor secreto, sin revelar ninguna información aparte del hecho de que conoce el valor secreto. Si bien esto requiere alguna entrada del verificador (por ejemplo, desafiar una respuesta), también existe una forma de este modelo llamada ZKP no interactivo, que no requiere tal interacción entre las dos partes.

Las aplicaciones que se benefician de ZKP son aquellas que requieren una medida de privacidad de datos. Algunas de estas aplicaciones de ejemplo incluyen:

- **Sistemas de autenticación**. El desarrollo de ZKP se inspiró en los sistemas de autenticación, en los que una parte necesitaba demostrar su identidad a una segunda parte a través de información secreta, pero sin revelar el secreto por completo.
- **Sistemas anónimos**. ZKP puede permitir que las transacciones de blockchain se validen sin la necesidad de revelar la identidad de los usuarios que realizan una transacción.
- **Sistemas confidenciales.** Al igual que los sistemas anónimos, ZKP se puede usar para validar transacciones de blockchain sin revelar información pertinente, como detalles financieros.

Zero-Knowledge Proofs (ZKP) permite el intercambio de información entre los participantes en las cadenas de valor al tiempo que conserva la capacidad de ajustar la cantidad de información divulgada. De esa manera, las cadenas de bloques se pueden usar para proporcionar un registro ultrarresistente de la procedencia de cualquier cosa que se pueda registrar en una base de datos, lo que permite conocer el nombre de la granja que cultivó los alimentos que consume, por ejemplo. O, en el caso de los procesos industriales, si el aluminio reciclado de un pedido procede realmente de una fuente de aluminio reciclado.

ZKP mantiene la información oculta indefinidamente, al tiempo que permiten que los usuarios de la cadena de bloques la interroguen. En lugar de enumerar todos los materiales de un componente, el ZKP actúa como un portal de preguntas y respuestas.

El modelo Zero-Trust de Ciberseguridad

El modelo Zero-Trust ha sido ampliamente reconocido como un enfoque eficaz para prevenir filtraciones de datos y mitigar el riesgo de ataques a la cadena

de suministro. Si bien este modelo ha sido ampliamente reconocido, su adopción en los sectores público y privado ha sido lenta e inconsistente.

Zero-Trust tiene como principio básico que no debemos confiar en nadie ni en nada solo porque está dentro del perímetro de la organización. Forrester estableció el modelo Zero-Trust que se centró en el principio rector "Nunca confíes, siempre verifica" y el reconocimiento de que los *firewalls* perimetrales ya no son suficientes para proteger los secretos comerciales y los activos.

Imagen: Tecnología mundial

Es importante reconocer que no existe un producto milagroso ni una forma única de implementar Zero-Trust. Requiere un enfoque de seguridad en capas que cubra toda la infraestructura digital, los sistemas heredados y modernos, con un enfoque en tener los controles adecuados donde el usuario accede a los recursos digitales y una menor dependencia de la seguridad del perímetro.

Si bien no existen definiciones comúnmente aceptadas, estos principios a continuación se reconocen como esenciales para implementar una hoja de ruta estratégica de Zero-Trust:

Principio 1: Coherencia en la forma en que autentica y autoriza a los usuarios y recursos digitales.
Principio 2: Asegurar todas las comunicaciones,

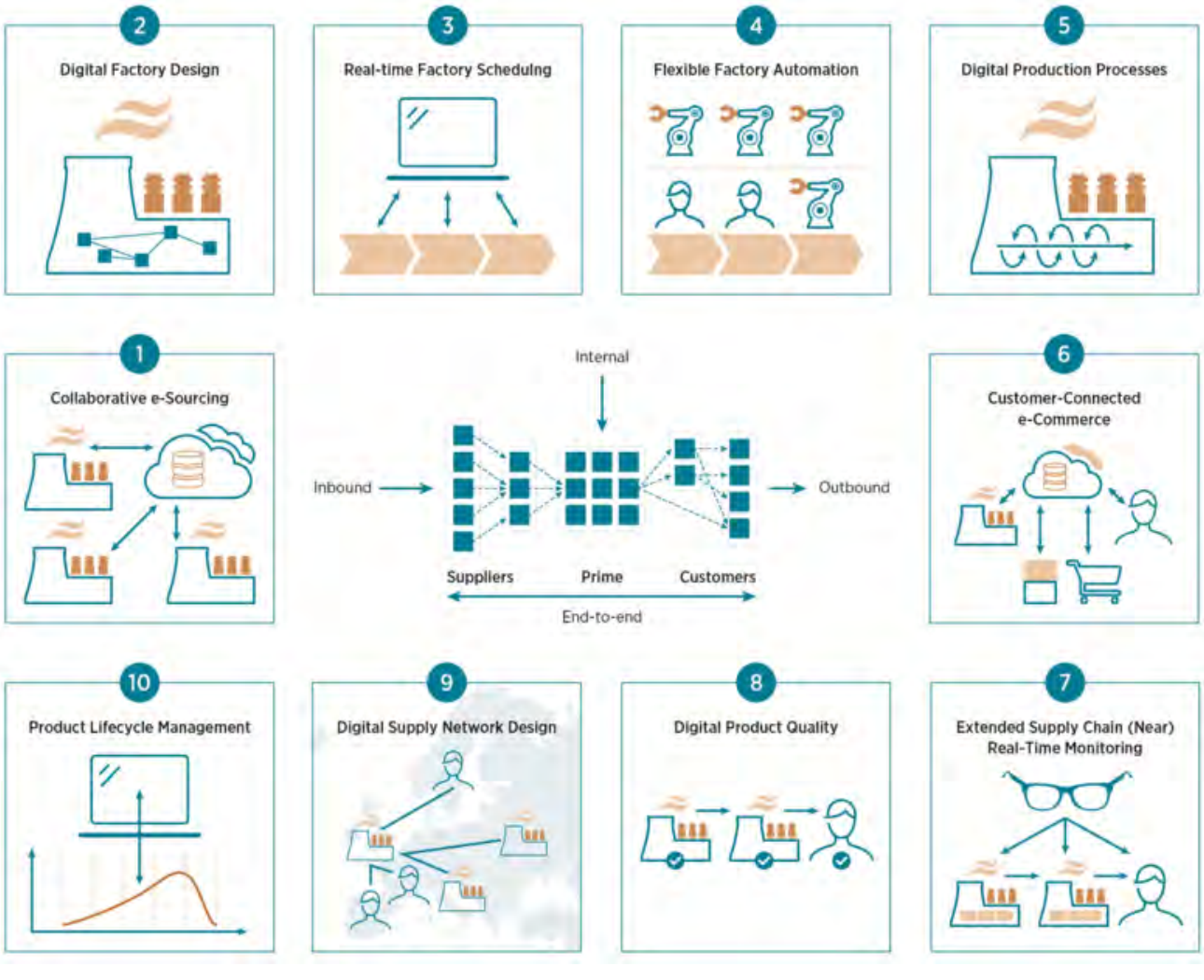


Imagen: Universidad de Cambridge - Las cadenas de suministro digitales son cada vez más complejas.

independientemente de la ubicación de la red.
Principio 3: Aplicar el acceso basado en el principio de privilegio mínimo.
Principio 4: Monitorear y verificar explícitamente la postura de seguridad y la integridad de todos los recursos digitales.
Principio 5: Consultar siempre los principios rectores "Nunca confíe, siempre verifique" y "suponga una infracción".

El componente de mayor valor de la cadena de suministro.

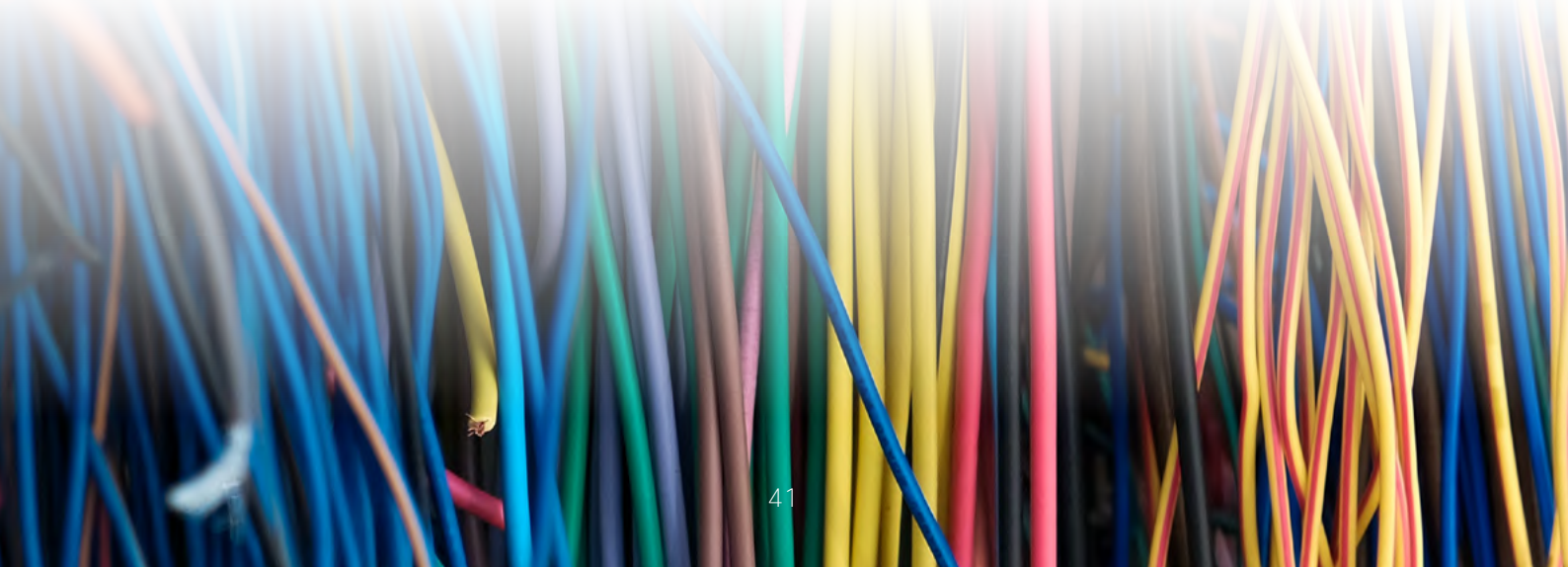
La implementación de tecnologías tales como el Blockchain, el ZKP y el Zero-Trust entre otras nos invita a pensar que las soluciones a los nuevos desafíos que se presentan con el desarrollo de la transformación digital y la industria 4.0 podrán tener un buen punto de equilibrio en relación a la ciberseguridad que estas tecnologías proveen. Como punto relevante de este equilibrio se presenta el componente humano, el eslabón más importante dentro de la protección y resguardo de la cadena de suministro, y a la vez, el más débil.

La carencia en América Latina y el Caribe de formación académica en Ciberseguridad es alta en términos de región, y muy dispar entre los diversos países de comprenden las subregiones del continente y así lo demuestra el Reporte de Ciberseguridad 2020 elaborado por la OEA y el BID. Según el informe, dos tercios de los países de América Latina y el Caribe presentan pocas o nulas mejoras en cuanto al nivel de madurez en materia de educación, capacitación y desarrollo de habilidades en ciberseguridad. Adicionalmente, oferta de formación especializada en seguridad digital en la mayoría de estos países es inexistente o tiene carácter de incipiente, y usualmente considera solo la dimensión técnica de la ciberseguridad.

En la búsqueda de una métrica que indique cuales podrían ser los niveles de avance en los diversos países de la región, nos encontramos que en pocos países se cuenta con algún tipo de levantamiento de información que demuestre el uso de los ambientes IoT – IIoT dentro de la cadena de suministro a nivel operacional, además se identifica que en ninguno de los países de la región se cuenta con un estudio que pueda demostrar el nivel de ciberseguridad de los ambientes hiperconvergentes aplicada en el uso de la cadena de suministro, por lo cual, el trabajo en este sentido apenas comienza.
Aprender es una virtud de los seres humanos, así que mantengamos siempre presentes las lecciones aprendidas y evitemos repetir experiencias como la adhesión definida en diversos países de LATAM de una normativa como la NERC-CIP que es aplicada como una solución para resguardar la Protección de Infraestructura Crítica - CIP y no como una normativa de ciberseguridad para el sector eléctrico (el mismo país creador de esta normativa reconoce que este no el objetivo para el cual fue concebida, y por esa razón actualmente desarrolla distintas iniciativas que son impulsadas tanto por el Departamento de Energía – DOE de los Estados Unidos como por CISA y tienen por objetivo desarrollar diversas leyes y normativas técnicas que sí tengan como foco la ciberseguridad de ese sector).

La generación de regulaciones que fortalezcan el marco jurídico de la cadena de suministro en el ámbito de la ciberseguridad es una necesidad que será altamente valorada en la región siempre que esta venga de la mano de planes de desarrollo de profesionales de ciberseguridad para los ambientes IoT – IIoT. De esta manera se evitará el vacío de capacidades humanas que generó la incorporación de regulaciones que no integraban el desarrollo de estas habilidades y que ahora sufren los diferentes equipos de recursos humanos de más de 1000 empresas del sector eléctrico en LATAM, que buscan personal en ciberseguridad sin hallarlo. Para un contexto como el actual, es muy baja la oferta de crecimiento profesional o académico que ayude a cubrir la demanda de personal creada en la región, así como tampoco personal con conocimiento empírico que acredite implementaciones de ciberseguridad como casos de éxito.

La creación de Estrategias de Ciberseguridad para las Infraestructuras Criticas de los países de la LATAM es el primer gran paso en la región



Especial
Trabajo híbrido

Abundancia y confusión, miedo e infidelidad

Imagen: Sharon Mccutcheon, Unsplash

Columna

por **Pablo Marrone**
Asesor en CX y Comunicación

Trabajar en tiempos de “cuasi post pandemia” y “cuasi tercera guerra mundial”. De eso se trata.

O ser líderes de equipo, en ese mismo contexto: sostener objetivos, inspirar horizontes, cautivar talentos.

En tiempos de miedo y confusión crecientes, la abundancia de tecnologías permite generar escenarios de trabajo diversos con el fin de atraer a empleados cada vez más infieles a sus propias organizaciones. La “gran renuncia” ha generado un desafío nunca visto.

La oferta del empleador debe pasar por generar una “experiencia del colaborador”, en la que su infraestructura de *hardware* y *software* sea la plataforma habilitante. Muy similar a lo que ocurre cuando navegamos la web, o vamos a un negocio y nos envuelven con la “experiencia del cliente”.

Con esa plataforma, dar opciones: algunos necesitan la seguridad y predictibilidad de la oficina. Otros la flexibilidad de poder elegir qué día estar aquí o allá. Todos necesitan convencerse de que eligen.

La pauta cultural fluye, como si fuera un reloj de Dalí y desafía a los líderes, que deben encontrar en esa fluidez su nueva zona de confort. Al mismo tiempo manejar las nuevas herramientas, e implementar las métricas imprescindibles para el negocio. Pero sin ser intrusivos.

El trabajo es híbrido, pero también la gestión y las interacciones. Estoy presente sin estar. Lidero sin ver. Cumplo sin alardear. Estoy disponible sin “micro gestionar”. Inspiro. Me dejo inspirar. Creo y ayudo a crear.

En tiempos de “post pandemia” y “cuasi tercera guerra mundial”, la fidelidad a la organización deriva de una experiencia humana y emocionalmente alineada con los colaboradores. El trabajo híbrido es una respuesta posible a esa necesidad de limitar la confusión y el miedo.

La oficina como espacio alternativo, la virtualidad colaborativa como valor, la tecnología como aliado invisible, amigable y transformador.

De eso se trata

Especial
Trabajo híbrido

Imagen: Sincerely Media, Unsplash.

Cumplir la promesa del trabajo híbrido

El trabajo híbrido es un enfoque que diseña la experiencia laboral en torno y para el trabajador donde se encuentre, lo que permite a las personas trabajar desde casa, en la oficina o en cualquier lugar. Es una evolución natural del trabajo remoto y representa una gran transformación de la cultura laboral. Además, permite a las organizaciones de hoy acentuar las fortalezas de su fuerza laboral y alinearse con sus estilos de trabajo preferidos, lo que da como resultado empleados más felices y productivos. Este documento examina cómo la convergencia de personas, tecnologías y lugares está impulsando el trabajo híbrido y los pasos a seguir para que esta modalidad funcione.

Imagen: Cristian Tarzi, Unsplash

El futuro de un trabajo aún más híbrido

Si bien la implementación práctica de las políticas de trabajo híbrido puede variar de una organización a otra y de una industria a otra, la mayoría de los trabajadores estarían de acuerdo en mantener la flexibilidad como política en el futuro. Esto se ilustra en la investigación de Cisco que reveló que solo el 9 % de los empleados quiere volver a la oficina a tiempo completo. La implicación es clara: el trabajo híbrido está aquí para quedarse y las organizaciones deben evolucionar sus modos tradicionales de operar para sobrevivir y prosperar en esta nueva era de trabajo.

La ventaja del trabajo híbrido

La buena noticia para las empresas es que muchos líderes han escuchado y planean prestar atención al llamado de atención del trabajo híbrido. La investigación muestra que 9 de cada 10 ejecutivos esperan un 38% de trabajo híbrido como modelo de hecho para sus empresas en el futuro.

Una visión clara hacia adelante

El mandato de acción hacia un futuro laboral más híbrido es claro, y muchas empresas y sus líderes lo han reconocido. Lo que es menos claro para estas empresas es la visión, la alineación y la experiencia necesarias para avanzar.

Qué sigue en el trabajo híbrido

Recursos para ayudarte a avanzar más y más rápido en la evolución del trabajo híbrido.

Hay varios recursos útiles disponibles para las empresas interesadas en desarrollar e implementar su propia estrategia de trabajo híbrido.

Cisco cuenta con una herramienta simple de preparación para el trabajo híbrido que proporciona una evaluación de la posición de una empresa hacia la viabilidad del trabajo híbrido en comparación con sus pares. La herramienta de evaluación también generará una guía detallada sobre temas como:

- Cómo optimizar el trabajo remoto.
- Cómo asegurar y administrar una infraestructura de trabajo híbrida.
- Cómo crear una cultura de trabajo inclusiva y solidaria.
- Cómo hacer que los empleados regresen a la oficina de manera segura.

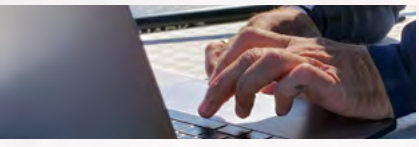
El índice de trabajo híbrido global de Cisco ha identificado tendencias de trabajo emergentes, al tiempo que muestra cómo las organizaciones pueden dar rienda suelta a la creatividad y la innovación, y mejorar el bienestar de sus trabajadores.

¿Alguna vez se preguntó cómo las empresas exitosas están haciendo la transición a nuevas formas de trabajar y cómo su organización se compara con los líderes de la industria? En junio de 2022, Cisco presentará el Modelo de madurez del trabajo híbrido para ayudar a las organizaciones a evaluar dónde se encuentran en sus viajes de trabajo híbrido y qué deben hacer para lograr sus objetivos. El modelo se basará en los resultados de encuestas de organizaciones de todos los tamaños y una variedad de industrias de todo el mundo. Examinará el espectro de madurez del trabajo híbrido a través de las etapas, comenzando con organizaciones que aún no han recorrido su camino, otras que han comenzado a implementarlo y aprender, hasta aquellas que realmente han adoptado un modelo de trabajo híbrido y, a través de su liderazgo, están impulsando el límites de lo que se puede lograr.

De los desafíos del trabajo híbrido a las oportunidades para la innovación

El cambio al trabajo híbrido marca un momento verdaderamente único para las organizaciones de todo el mundo que pueden redefinir todos los aspectos del trabajo para crear entornos de trabajo más flexibles, que incluyan apoyo, administración y seguridad. Esta tendencia generacional está impulsada por la convergencia de personas, tecnología y lugares y está remodelando permanentemente las expectativas tanto de los empleadores como de los empleados.

Si bien el cambio al trabajo híbrido presenta varios desafíos, las organizaciones que toman medidas significativas ahora tienen la oportunidad de impulsar la inclusión, mejorar la productividad y permitir la interactividad a niveles sin precedentes. Esto dará como resultado empleados más felices y productivos, lo que puede crear organizaciones más fuertes que lideren en esta próxima era de trabajo



Alineación C-level

Cómo generar claridad en torno a la visión de trabajo híbrido

El mandato de acción hacia el trabajo híbrido es claro y muchas organizaciones y sus líderes lo han reconocido. Lo que no está tan claro es qué pasos deben tomar estas empresas para avanzar. Un informe reciente (1) ilustra esto con nueve de cada diez ejecutivos que dicen que visualizan un modelo de trabajo híbrido en el futuro mientras solo tienen un plan básico de alto nivel para seguir adelante. De hecho, un tercio de estas empresas dice que sus organizaciones "carecen de alineación en una visión de alto nivel entre el equipo superior" y "solo una de cada diez organizaciones ha comenzado a comunicar y probar esa visión".

Esto presenta una oportunidad para los líderes y sus equipos en funciones clave como la estrategia tecnológica, la gestión de personas y las operaciones para ayudar a impulsar la visión de trabajo híbrido en sus organizaciones. Aquí presentamos un resumen de esas oportunidades por función:

CIO:

El trabajo híbrido está creando una convergencia de tecnologías de colaboración, redes y seguridad. Nuestros empleados necesitan un acceso fluido a aplicaciones y experiencias colaborativas de alta calidad, lo que hace que sea fundamental proteger las herramientas de trabajo remoto para resguardar los datos de los clientes y empleados en todo momento. Los CIO pueden desempeñar un papel central para ayudar a sus empresas a navegar por las estrategias digitales de colaboración, redes, seguridad y otras. Esto dará como resultado organizaciones más ágiles y con conocimientos digitales que pueden satisfacer mejor las necesidades de los empleados, clientes y socios.

CHRO:

Comprender las necesidades y expectativas de nuestros empleados es fundamental para retener a los mejores talentos y expandir el grupo. Los empleados de hoy quieren más flexibilidad y más voz sobre dónde, cuándo y cómo trabajan. Pero no hay una talla única para todos. Las experiencias laborales, los estilos de trabajo y las preferencias laborales son tan variadas y personales como las personas que componen la fuerza laboral de una organización. Al escuchar a los empleados y permitir que los equipos determinen las configuraciones de trabajo híbridas que funcionan mejor para ellos, las empresas pueden capacitar a su gente y equipos para que aprovechen sus fortalezas y se concentren en hacer que el trabajo funcione para ellos.

COO:

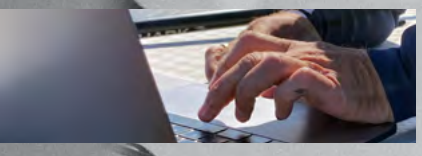
El trabajo híbrido redefinirá significativamente la gestión de las operaciones y las instalaciones, especialmente cuando los empleados vuelvan a trabajar a gran escala. Garantizar la seguridad y la productividad de los empleados son las principales prioridades, lo que requiere rediseñar nuestros lugares de trabajo para que se centren más en el ser humano y menos en la oficina. Esto incluirá la construcción de espacios de colaboración dedicados e "inteligentes" para conferencias más fáciles y menos espacios de trabajo asignados o más pequeños. Por lo tanto, el director de operaciones puede desempeñar un papel integral para ayudar a crear un lugar de trabajo "centrado en el ser humano" que sea fundamental para el desempeño híbrido.

A medida que desarrolla la estrategia de trabajo híbrido para cada organización, Cisco sugiere utilizar las siguientes cinco características (2) que pueden servir como un marco útil o una lista de verificación para crear soluciones de este tipo de labor:

Inclusivo: igualdad de experiencias para todos.
Flexible: adaptándose a cualquier estilo de trabajo, rol, entorno.
De apoyo: centrándose en la seguridad, la empatía y el bienestar.
Seguro: ser seguro por diseño, privado por defecto.
Administrado: entrega de infraestructura moderna, administración sin fricciones

(1) **McKinsey & Company:** lo que dicen los ejecutivos sobre el futuro del trabajo híbrido, mayo de 2021.
(2) **Cisco:** ¿Qué es el trabajo híbrido? Características del Trabajo Híbrido, 2021.

Imagen: Marten Bjork, Unsplash.



Especial
Trabajo híbrido

Cinco tips
para mantenerlo seguro

A medida que el mundo hace la transición hacia una fuerza laboral híbrida permanente, la flexibilidad trae nuevos beneficios y desafíos para empleadores y trabajadores. Ya sea que el equipo esté trabajando en la oficina, de forma remota o bajo un esquema intermedio, es preciso no comprometer la seguridad. Aquí compartimos una lista de cinco consejos simples para mantener la cultura de fuerza laboral híbrida, mientras se protege a los trabajadores y a los activos de la empresa.

Imagen: Charlesdeluvio, Unsplash.

01

Educar a la fuerza laboral para que adopte prácticas laborales seguras

Los trabajadores esperan que la tecnología los siga dondequiera que vayan, pero tener ubicaciones flexibles los expone a ellos (y a su organización) a amenazas de formas nuevas. Es por eso que los equipos de TI y seguridad deben garantizar que la experiencia híbrida sea segura en todos los puntos finales al educar a los usuarios sobre prácticas seguras y peligros potenciales.

02

Verificar que la persona es quien dice ser

La autenticación multifactor (MFA) es una primera capa de seguridad simple que todas las empresas necesitan antes de poder otorgar acceso a los activos de la empresa. Se trata de un método de control de acceso informático en el que a un usuario se le concede acceso al sistema solo después de que presente dos o más pruebas diferentes de que es quien dice ser, con el objetivo de verificar su identidad y el estado del dispositivo.

03

Habilitar el acceso seguro desde cualquier lugar

VPN (Virtual Private Network) proporciona un túnel seguro entre los usuarios y las aplicaciones para que los trabajadores puedan mantenerse productivos y conectados cuando están de viaje o trabajando desde casa. Ayuda a garantizar que solo ingresen los usuarios aprobados al proporcionar el nivel adecuado de seguridad sin comprometer la experiencia del usuario.

04

Adoptar la defensa contra las amenazas de seguridad en cualquier punto de entrada

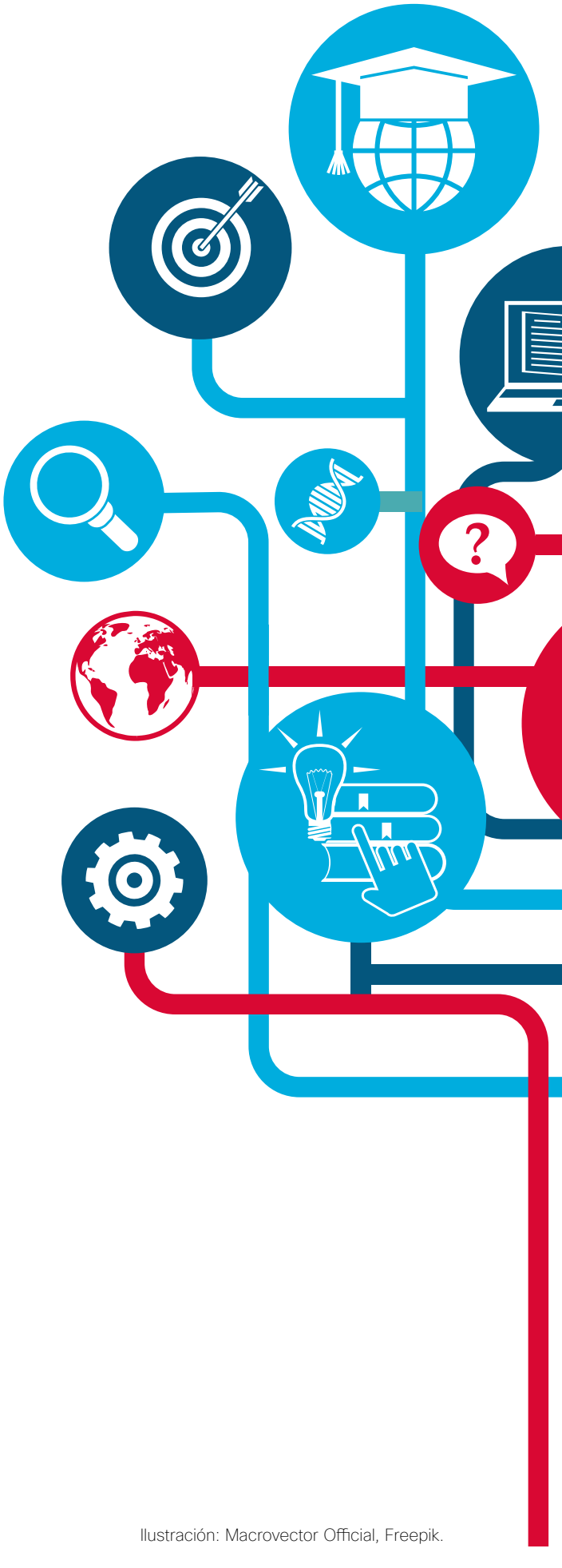
La mayoría de las infracciones de seguridad tienen como objetivo a los usuarios finales, lo que requiere una primera línea de defensa en la capa de DNS y una última línea para las amenazas que se filtran. La primera capa bloquea los dominios asociados con el comportamiento malicioso antes de que ingresen a su red o contengan *malwares* si ya está dentro, mientras que la última capa protege contra amenazas más avanzadas.

05

Unificar la seguridad a través de una plataforma simple e integrada

Buscar que la seguridad sea fácil y efectiva es una vía que colabora en la gestión integral. A través de la plataforma SecureX, los productos Cisco Secure y la infraestructura se unen y contribuyen a una administración de seguridad simple y efectiva.

Con Cisco Secure Hybrid Work es posible mantener los datos seguros donde sea que trabajen las personas que forman parte de la organización, ya que se trata de una solución simple y unificadora para habilitar la seguridad en todas partes y potenciar el trabajo en cualquier lugar



¿Por qué un programa de formación online sobre ciberseguridad?

La Ciberseguridad es una especialidad que ha ido adquiriendo importancia en función de la transformación tecnológica experimentada por instituciones y empresas, y cuya finalidad última consiste en proteger los activos digitales - equipos de trabajo, información, servicios en Internet, redes de comunicaciones, etc.- de amenazas que comprometan su confidencialidad, integridad y disponibilidad. Hoy en día las empresas no se cuestionan si van a ser víctimas o no de un ciberataque, simplemente tienen que estar preparadas para cuando les toque.

¿Cuál es el objetivo del programa?

El objetivo del Programa neddux online en Ciberseguridad, es doble:

1. Transmitir los conocimientos necesarios para entender el alcance y la relevancia de esta materia y

2. Aplicar ese conocimiento en la gestión de las situaciones y en la resolución de los problemas que se plantean.

Para ello, se han diseñado dos modalidades teniendo en cuenta los diferentes perfiles de empleados que hay en una organización y que, por tanto, requieren una formación diferenciada:

Ilustración: Macrovector Official, Freepik.

Sección
Capacitación

Cisco Secure, a través de la empresa neddux, impartirá un programa de formación en ciberseguridad para líderes de la región. En una conversación amena, **Eduardo Gómez**, CEO de neddux comparte con Bridge los lineamientos de esta capacitación.

1.- Programa de Gestión: dirigido a responsables del área de Sistemas, de Ciberseguridad, y al primer nivel directivo, que deben afrontar la toma de decisiones prudenciales. Está compuesto de seis módulos formativos que abarcan todas las fases claves para gestionar la Ciberseguridad, siguiendo la metodología del caso. Tiene una duración aproximada de 45 horas, que se distribuyen de forma autónoma a lo largo de tres meses.

2.- Programa de Sensibilización, dirigido a todas las personas que manejan activos, equipos, información, servicios, redes de comunicación, etc., su objetivo es sensibilizar sobre la importancia del manejo adecuado y evitar el camino de entrada a los ciberdelincuentes por desconocimiento. Tiene una duración de una hora.

¿Cuáles son los beneficios de este programa de formación que lo hace diferente a otros?

El programa de neddux y la Universidad Francisco de Vitoria tiene características propias y desarrolla una metodología que no existe actualmente en el ámbito de la formación online:

Utiliza el cine académico:
La producción personalizada de cine, basado en experiencias y casos reales de ciberataques, que permite al alumno vivir la experiencia como un protagonista más de la película, despertando una parte del cerebro que normalmente está dormida en los procesos de aprendizaje tradicionales. El cine se aplica también en cada una de las fases de la metodología neddux: trabajo en equipo, diagnóstico y toma de decisiones. El alumno mantiene el interés y entra en la materia académica de forma progresiva, casi sin darse cuenta, afianzando los conceptos de una forma natural y sencilla y aplicándolos a una realidad concreta. El cine académico es solo el primer paso, aunque muy importante, dentro de la metodología neddux.

El rigor académico del método del caso:
El programa está basado en el método del caso, que se aplica en las mejores escuelas de negocio del mundo. El alumno tiene la oportunidad de recorrer todas las fases de esta metodología mejorando su capacidad de análisis, de síntesis, de diagnóstico, de generar alternativas de acción, valorarlas y por último, tomar decisiones. Esto mejora su proceso de toma de decisiones y le permite afrontar los problemas de futuro con mayor competencia.

Autoaprendizaje: todo el contenido académico se ha encapsulado en un formato flexible, que se puede adaptar a la disponibilidad de tiempo que tienen los alumnos para su estudio. Esta flexibilidad se consigue porque incorporamos el cine a otros elementos clave del método del caso como son el trabajo en equipo, la clase del profesor y la toma de decisiones, por ejemplo. Hemos incrementado el valor de la formación online mediante el cine académico.

Contenido del Programa de Gestión

El *"Programa de gestión de la ciberseguridad"* es una especialidad que consta de 6 módulos independientes presentados de forma progresiva con el siguiente orden:

Gestión de los riesgos en materia de ciberseguridad. Se identifican los principales conceptos de riesgo que permiten entender una disciplina como la ciberseguridad, que pivota en torno al conocimiento de los activos, las vulnerabilidades, las amenazas, los riesgos potenciales, controles, etc.

Security Operation Center (SOC). En este módulo se detectan las actividades hostiles contra las infraestructuras tecnológicas y sus servicios, y la gestión de las alertas asociadas.

Vulnerabilidades y revisiones de ciberseguridad. El programa avanza revisando las vulnerabilidades, que son debilidades de control o errores en los sistemas que ponen en riesgo la seguridad de la información y de los servicios.

Incident Response Plan. En este módulo se profundiza en el plan de respuesta ante incidentes, que es un conjunto ordenado de acciones enfocadas a dar respuesta a un incidente con altos niveles de criticidad e impacto en las operaciones y funciones de negocio.

Plan Director de Ciberseguridad. El quinto módulo revisa la importancia de tener diseñado un plan, explica la forma de elaborarlo y los elementos clave que debe estar presentes para reducir o mitigar los riesgos.

Frameworks de ciberseguridad. Para finalizar, se presenta la necesidad de contar con un marco de referencia, que contenga el conjunto de mejores prácticas, actividades estructuradas, controles, evaluaciones y mediciones, de tal forma que exista una cultura transversal en materia de ciberseguridad.

Contenido del Programa de Sensibilización

El *"Programa de sensibilización de la ciberseguridad"* es un curso apoyado principalmente en la película y en el que se resuelven cuestiones básicas para entender la importancia de ser prudentes a la hora de gestionar activos de la empresa.

El valor que aporta el grupo, clave para mantenerse al día

Más allá de tratarse de un programa basado en la autoformación, los participantes forman parte de una promoción de 25 alumnos en la que van a poder compartir sus experiencias en dos momentos a lo largo de cada uno de los 6 módulos: en el trabajo en equipo, formado por 5 alumnos cada uno, y en las sesiones plenarias que imparte el profesor al finalizar el estudio de cada módulo.

Los ciberdelincuentes están continuamente innovando sobre cómo hacer el mal y van siempre por delante. Este programa está diseñado para contrarrestar esa ventaja mediante la puesta en común de las experiencias vividas, apoyados en el conocimiento y la amplia experiencia del equipo docente

ÚNETE A WOMCY

Somos una organización sin fines de lucro, conformada por mujeres, con foco en el desarrollo de la Ciberseguridad en América Latina.

WOMCY

LATAM Women in Cybersecurity

www.womcy.org

Imagen: Timon Studler, Unsplash.

La privacidad se convierte en una misión crítica

Estudio comparativo de privacidad de datos, Cisco 2022

Introducción

En los últimos años, la privacidad se ha convertido en una misión crítica para las organizaciones de todo el mundo. Más de dos tercios de los países han promulgado leyes de privacidad, los clientes no compran a organizaciones que no protegen sus datos y las métricas de privacidad se informan regularmente a las juntas directivas. Además, las habilidades de privacidad son cada vez más importantes, especialmente entre los profesionales de la seguridad, y las organizaciones se benefician financieramente de sus inversiones en esta materia. Este informe, nuestra quinta revisión anual de cuestiones clave de privacidad para las organizaciones, examina el impacto de la privacidad en las empresas de todo el mundo.

Puntos clave del informe

1. La privacidad se ha vuelto esencial para la cultura y las prácticas comerciales de las organizaciones, incluidos sus procesos de compra, métricas de gestión y áreas de responsabilidad de los empleados.
2. El retorno de la inversión (ROI) de la privacidad sigue siendo alto por tercer año consecutivo, con mayores beneficios, especialmente para las organizaciones pequeñas y medianas y un ROI más alto para las organizaciones más maduras en privacidad.
3. La mayoría de las organizaciones reconocen su responsabilidad de tratar los datos de manera ética, pero muchos clientes quieren más transparencia y están preocupados por el uso de los datos, en particular en la inteligencia artificial (IA) y la toma de decisiones automatizada.
4. Los requisitos de localización de datos se consideran importantes pero costosos.
5. Alinear la privacidad con la seguridad parece crear ventajas financieras y de madurez, en comparación con otros modelos organizacionales.

Metodología

Los datos de este estudio se derivan de la encuesta Cisco Security Outcomes, en la que los encuestados eran anónimos para los investigadores y no se les informaba quién estaba realizando el relevamiento. Usando la misma metodología que en años anteriores, más de 5300 profesionales de seguridad de 27 geografías completaron la encuesta en el verano de 2021. Los encuestados representan todas las industrias principales y una combinación de tamaños de empresas (consulte el Apéndice 1). Dirigimos preguntas específicas sobre privacidad a los más de 4900 encuestados que indicaron estar familiarizados con los procesos de privacidad en sus organizaciones. En este informe, también hemos incluido resultados relevantes de la Encuesta de privacidad del consumidor de Cisco 2021, que fue completada en el verano de 2021 por 2600 adultos en 12 países.

1. La privacidad se convierte en una misión crítica

La privacidad se ha convertido en un imperativo comercial y un componente crítico de la confianza del cliente para las organizaciones de todo el mundo. Por segundo año consecutivo, el 90 % de los encuestados en nuestra encuesta global dijo que no comprarían de una organización que no protege adecuadamente sus datos, y el 91 % indicó que las certificaciones de privacidad externas son importantes en su proceso de compra.

La pandemia de COVID-19 fortaleció aún más el papel de la privacidad, ya que el 91 % de las organiza-

ciones dijo que sus equipos de privacidad las ayudaron a lidiar con muchos problemas complejos de datos personales de la fuerza laboral que surgieron en los últimos años. Quizás no sea sorprendente entonces que el 92 % de las organizaciones dijera que respetar la privacidad es parte integral de su cultura.

Nuestros clientes no nos comprarían si no protegiéramos adecuadamente sus datos 90 %

Las certificaciones de privacidad externas son un factor en nuestro proceso de compra 91 %

La privacidad es parte integral de nuestra cultura 92 %

Visión fuertemente favorable de las leyes de privacidad

La legislación sobre privacidad sigue siendo muy bien recibida en todo el mundo. Estas leyes desempeñan un papel importante al proporcionar garantías de que los gobiernos y las organizaciones rindan cuentas por la forma en que gestionan los datos personales, y más de dos tercios (128 de 194) de los países ya cuentan con leyes de privacidad. Aunque cumplir con estas leyes a menudo implica un esfuerzo y un costo significativos (por ejemplo, catalogar datos, mantener registros de actividades de procesamiento, implementar controles - privacidad por diseño, responder a las solicitudes de los usuarios), las organizaciones reconocen el impacto positivo. Ochenta y tres por ciento de todos los encuestados corporativos dijeron que las leyes de privacidad han tenido un impacto positivo, el 14 % fueron neutrales, y solo el 3 % indicó que las leyes han tenido un impacto negativo. A pesar de la complejidad adicional provocada por más legislación durante el año pasado, este resultado es aún más po-

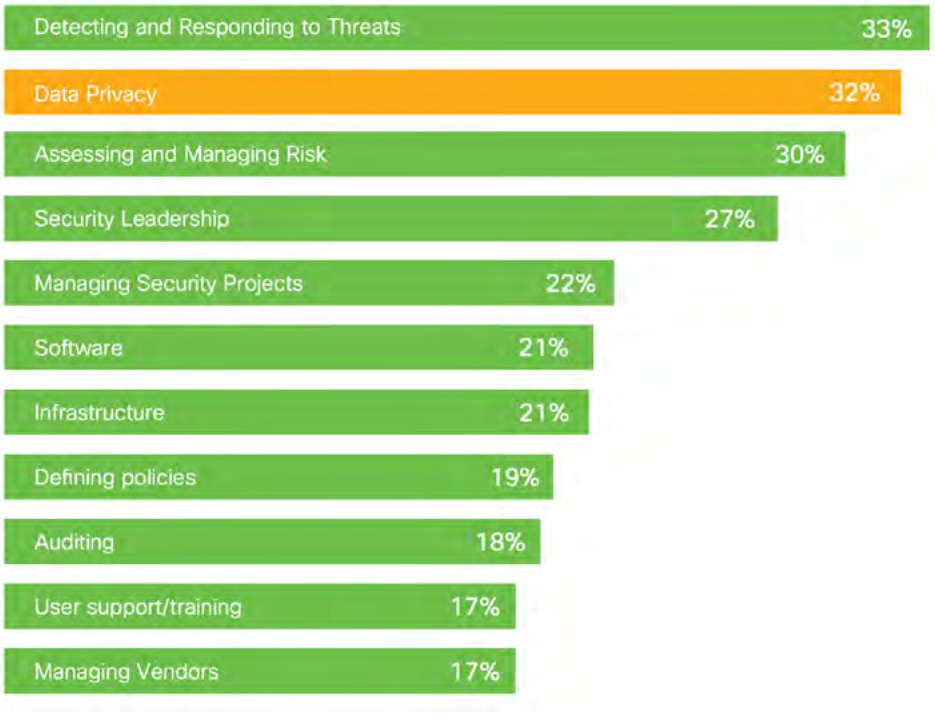
sitivo que en la encuesta del año pasado (donde los encuestados fueron 79 % positivos, 7 % negativos). También cabe destacar lo fuerte que es esto en todo el mundo. En muchas geografías, incluidas Filipinas, México, Tailandia, Indonesia, China y Vietnam, el 90 % o más de los encuestados dijo que la regulación de la privacidad ha tenido un impacto positivo, y en cada geografía de nuestra encuesta, al menos dos tercios de los encuestados indicaron lo mismo. Consulte la *Figura 2*. Como se discutió en nuestros informes anteriores, tanto los consumidores como las organizaciones esperan y valoran un rol gubernamental sólido en la protección de la privacidad. Las reglamentaciones pueden proporcionar un estándar de atención más consistente, mayor claridad sobre los derechos y recursos de los propietarios de datos y pautas sobre qué actividades de procesamiento de datos están permitidas o prohibidas.

La gran mayoría está informando las métricas de privacidad a su Junta Directiva

Una indicación importante de la importancia de la privacidad para la organización es el uso de métricas de privacidad, especialmente cuando se informan a la dirección ejecutiva y al Directorio. Entre las organizaciones en la encuesta de este año, el 94% informa una o más métricas relacionadas con la privacidad a la Junta. Mientras que algunos informan hasta 10 métricas de privacidad, la mayoría informa entre 1 y 3, con un promedio general de 2,6. Las métricas más informadas incluyen los resultados de la auditoría del programa de privacidad (34 %), las infracciones de datos personales (33 %) y los resultados de las evaluaciones de impacto de la privacidad (32 %).

La privacidad es un área central de responsabilidad para profesionales de la seguridad

Las habilidades de privacidad se han vuelto cada vez más críticas, especialmente entre aquellos que son directamente responsables de mantener la seguridad de los datos. Se pidió a los profesionales de seguridad que completaron nuestra encuesta que definieran sus 3 principales áreas de responsabilidad. “Privacidad y gobernanza de datos” fue seleccionado por el 32 % de estos encuestados, lo que lo coloca en segundo lugar después de “Detectar y responder a amenazas” y justo por delante de “Evaluación y gestión de riesgos”. Consulte la Figura 4. La privacidad de los datos se ha convertido en una competencia central para



estos equipos de seguridad, y la integración de las habilidades de privacidad puede ayudar a garantizar que aquellos que están autorizados a acceder a los datos los manejen de manera adecuada.

Curiosamente, varias geografías de Asia-Pacífico tuvieron el porcentaje más alto de encuestados en los que la privacidad se identificó como un área de responsabilidad, es decir, Indonesia (45 %), Vietnam (43 %), India (43 %) y Malasia (42 %). Los porcentajes más bajos se dieron en Chile (19 %), Francia (22 %), Colombia (23 %) y el Reino Unido (24 %). Consulte la Figura 5. Las diferencias pueden reflejar una mayor integración entre la seguridad y la privacidad en muchos países de Asia-Pacífico. También puede deberse a organizaciones en países con regímenes de privacidad más antiguos que asignan responsabilidades de privacidad a áreas distintas a la función de seguridad, pero se necesitará más investigación sobre este tema.

2. Inversión y beneficios de privacidad

A medida que la privacidad se integra más en las prioridades organizacionales, la inversión continúa aumentando. El presupuesto de privacidad promedio aumentó un 13 %, de $2,4 millones el año pasado a $2,7 millones este año. El gasto en organizaciones más pequeñas de 50 a 249 empleados aumentó de $1,1 millones a $1,7 millones, y aquellas con 250 a 499 empleados aumentaron de $1,6 millones a $2,1 millones. Mientras tanto, las organizaciones más grandes (más de 10.000 empleados) vieron una ligera disminución en el gasto de $3,7 millones a $3,5 millones este año después de un fuerte aumento el año pasado. En investigaciones futuras, exploraremos de donde proviene el crecimiento del gasto, ya sea el número de empleados, la tecnología o el asesoramiento externo.

El valor comercial asociado con estas inversiones sigue siendo alto. Noventa por ciento de todos los encuestados dijeron que consideran la privacidad un imperativo empresarial. Más específicamente, preguntamos a los encuestados sobre los beneficios potenciales en 6 áreas: reducir los retrasos en las ventas, mitigar las pérdidas por filtraciones de datos, permitir la innovación, lograr la eficiencia operativa, generar confianza con los clientes y hacer que su empresa sea más atractiva. Para cada una de estas seis áreas, más del 60 % de los encuestados sintieron que estaban obteniendo beneficios significativos o muy significativos, y esta medida ha sido ampliamente consistente durante los últimos dos años.

También se pidió a los encuestados que estimaran el valor financiero de los beneficios de sus inversiones en privacidad, y la estimación promedio aumentó un 3 %, de $2,9 millones el año pasado a $3,0 millones este año. Curiosamente, las organizaciones más pequeñas vieron los mayores aumentos porcentuales este año. Aquellos con 50-249 empleados aumentaron de $1,1 millones a $2,0 millones, y aquellos con 250-499 empleados aumentaron de $1,9 millones a $2,5 millones. Los beneficios en organizaciones con 1000-9999 empleados se mantuvieron constantes en $3,4 millones y en las organizaciones más grandes con más de 10.000 empleados, los beneficios cayeron levemente de $4,0 millones a $3,8 millones.

El ROI disminuye levemente, pero se mantiene fuerte

Desde una perspectiva de retorno de la inversión, la organización promedio estimó los beneficios en 1,8 veces el gasto, que es inferior al 1,9 de la encuesta del año pasado. Creemos que esto se debe a las necesidades continuas de respuesta a la pandemia, la adaptación a la nueva legislación, la incertidumbre sobre las transferencias internacionales de datos y el aumento de los requisitos para la localización de datos. No obstante, la mayoría de las organizaciones continúa obteniendo un rendimiento muy atractivo de sus inversiones en privacidad. El 32 % de las organizaciones obtienen beneficios de al menos el doble de lo que gastan, y solo el 19 % estima que no alcanza el punto de equilibrio en sus inversiones en privacidad.

Rendimientos más altos para organizaciones más maduras y donde la privacidad se integra con la seguridad

También es interesante observar las correlaciones entre el rendimiento y otros factores como la madurez de la privacidad. Los encuestados que sintieron que su programa de privacidad estaba por debajo del de sus pares estaban obteniendo un retorno menor que aquellos que sintieron que estaban igual o por delante de sus pares. En concreto, los menos maduros tuvieron una rentabilidad media de 1,53, frente a una rentabilidad media de 1,97 de los más maduros. Esto demuestra aún más el valor de la inversión en privacidad, ya que las organizaciones más maduras también obtienen los mayores beneficios.

Otra correlación relevante fue entre el rendimiento de la privacidad y si el encuestado identificó la privacidad como una responsabilidad central de su trabajo como profesionales de la seguridad. Las organizaciones donde el encuestado identificó la privacidad como una responsabilidad tuvieron un rendimiento promedio de casi 2x en comparación con 1,71x donde el encuestado no identificó la privacidad.

Este resultado sugiere que hay un valor comercial en tener privacidad y seguridad trabajando de la mano.

3. Ética de datos y toma de decisiones automatizada

La inteligencia artificial (IA) y la toma de decisiones automatizada plantean desafíos particulares para las organizaciones y los consumidores con respecto al uso de datos personales. Noventa y dos por ciento de los encuestados reconoce que su organización tiene la responsabilidad de usar los datos solo en una manera ética. Y casi la misma cantidad (87 %) cree que ya tiene procesos implementados para garantizar que la toma de decisiones automatizada se realice de acuerdo con las expectativas del cliente. Los consumidores no están de acuerdo. Basándose en los resultados de la Encuesta de privacidad del consumidor de Cisco 2021, casi la mitad (46 %) de los consumidores sienten que no pueden proteger adecuadamente sus datos, y la razón principal es que no entienden exactamente lo que las organizaciones recopilan y hacen con sus datos.

Los consumidores valoran la transparencia cuando se trata de cómo se utilizan sus datos, y la toma de decisiones con IA puede ser particularmente difícil de explicar. De hecho, el 56 % de los encuestados expresó su preocupación sobre cómo las empresas utilizan la IA en la actualidad. Además, cuando se les preguntó sobre el uso de datos personales en varios casos de uso típicos de IA (ej., selección de un representante de ventas, establecimiento de precios, determinación de la solvencia), un gran porcentaje, que va del 37 % al 55 %, dijo que confía menos en una empresa que utilizó IA para estas decisiones. Consulte la Figura 12. Las organizaciones deben hacer más para asegurarse de que los clientes comprendan cómo se utilizan sus datos y generan confianza. Esto probablemente será un desafío importante con respecto a las decisiones basadas en IA.

4. Localización de datos

A medida que los gobiernos y las organizaciones continúan exigiendo protecciones y compromisos para los datos transferidos fuera de sus fronteras nacionales, más están implementando requisitos de localización de datos. En una nueva área de investigación este año, el 92 % de los encuestados dijo

que esto se ha convertido en un tema importante para sus organizaciones, y el mismo porcentaje indicó que cree que es necesario para ayudar a proteger los datos personales. Pero tiene un precio. Ochenta y ocho por ciento dijo que los requisitos de localización están agregando un costo significativo a su operación.

Si bien este requisito a menudo es impulsado por las leyes y actitudes nacionales, no hubo una variación sustancial entre los encuestados en diferentes geografías. El porcentaje de encuestados que dijo que la localización de datos estaba agregando costos a su operación estaba entre el 77 % y el 94 % en todas las geografías.

5. Opciones organizacionales para la privacidad

En los ejercicios de evaluación comparativa, los profesionales de la privacidad están particularmente interesados en comprender dónde se encuentra la función de privacidad dentro de otras organizaciones y dónde podría ser mejor encajar. Entre los encuestados en nuestra encuesta, no parecía haber un modelo dominante. La privacidad se ubicó con mayor frecuencia en TI (37 % de los encuestados), seguida de Seguridad, Cumplimiento, Legal y Operaciones.

En cuanto a dónde podría encajar mejor, un factor sería qué modelo es consistente con los rendimientos estimados más altos de la inversión en privacidad. Entre los encuestados, el retorno promedio más alto fue entre las organizaciones donde la Privacidad se encuentra en Seguridad, con un retorno de 1,91. Los ubicados en TI tuvieron una rentabilidad promedio de 1,87 y los de Legal 1,77.

Desde el punto de vista de la madurez de la privacidad, era más probable (43 %) que aquellos en los que la Privacidad se ubica en Seguridad dijeran que estaban por delante de sus competidores, en comparación con aquellos en los que la Privacidad se ubica en TI (37 %), Legal (37 %), Cumplimiento u Operaciones. Estas correlaciones nuevamente sugieren que existe un valor comercial significativo a partir de una integración más estrecha entre privacidad y seguridad.

Recomendaciones

La privacidad continúa integrándose en las prioridades organizacionales, y los hallazgos de esta investigación apuntan a recomendaciones específicas sobre cómo demostrar confianza y maximizar los beneficios de las inversiones en privacidad, que incluyen:

1. Continúe desarrollando capacidades de privacidad en toda su organización, particularmente entre los profesionales de seguridad y TI y aquellos que están directamente involucrados con el procesamiento y la protección de datos personales.

2. Sea transparente acerca de cómo los productos y servicios que ofrece su organización utilizan los datos personales. Los clientes quieren saber, y estar seguros, de que sus datos no están siendo abusados ni utilizados de formas que no esperan, conocen o entienden.

3. Proceda con cuidado y consideración al usar datos personales en IA y toma de decisiones automatizada que afecte materialmente a los clientes. Diseñar y construir con un marco ético, establecer la gobernanza y la supervisión de su programa de IA y brindar transparencia sobre cuándo y cómo está utilizando la toma de decisiones automatizada son todos los pasos positivos que las organizaciones pueden tomar.

4. Invierta en privacidad: ¡vale la pena!

Cisco continuará monitoreando estas tendencias y problemas y compartirá sus hallazgos. Para obtener información adicional sobre la investigación de privacidad de Cisco, comuníquese con Robert Waitman, director de investigación y economía de privacidad de Cisco, en rwaitman@cisco.com
Accede al estudio completo con las figuras y el apéndice desde aquí.


CISCO
SECURE