Número 1. 2024

IMPACTO

by OCP TECH

DOSSIER
Smart Cities

CONVERSATORIO
El valor de la voz
en la experiencia del cliente

DUPLAS
Fraude y Ciberseguridad

Versión Digital


OCP
TECH
INGENIERÍA DE IMPACTO

De aceleraciones y reencuentros

El mundo de las tecnologías y lo corporativo nos vincula, desde hace ya tiempo, a ritmo acelerado. De por sí, su propia característica expansiva retroalimenta su crecimiento y velocidad.

Y aquí estamos nosotros, todavía poniendo el cuerpo -pandemia y distanciamiento de por medio- en un mundo que ha sabido sostener una crisis global a través de los desarrollos de las TIC, y que modificó gran parte de las dinámicas sociales, económicas y culturales de una forma que seguramente en unos años podamos ver con más claridad.

Sabemos que los nuevos desarrollos nos encuentran con una infraestructura cada vez más grande sobre la cual trabajar, que intensifica nuestra labor y diversifica cada vez más nuestras tareas. Esto último nos puede hacer sentir, entre *"pendings"* y deseos, cierta sensación de vértigo, por eso, nos invito a hacer conexiones y pensar en lo importante, lo urgente y lo necesario.

IMPACTO by OCP TECH surge como una respuesta a la necesidad de poner un freno y mirar a nuestro alrededor, ampliar la visión y tomar perspectiva. Vivimos en un ecosistema integrado con la tecnología que debe tener, necesariamente, un retorno hacia las personas; la única forma de acercar soluciones y generar impacto debe ser expandiéndonos sin perder el foco en lo humano, siendo conscientes de la repercusión social que podemos generar.

Sabiendo eso, esta revista se vuelve material para todos, desde estudiantes hasta ejecutivos, quienes quieran poner el *switch* en *"reset"* y hacer uso de un espacio de lectura e interpelación para, de alguna forma, reencontrarnos en el camino.

Flor Palazzolo
Strategic Communications Director

OCP TECH Latinoamérica

Founder and CEO
Leonardo Scatturice

COO
Andrés Quinn

CFO
Fernando Antolín Dulac

Regional Sales Director NOLA & Caribbean
Cesar Calderón

VP Sales NOLA
Hernán Piñero

VP Sales SOLA
Jorge Pinjosovsky

CLO
Josefina Eizayaga

Compliance Officer
Lucio Primucci

CIO
Ariel Castaño

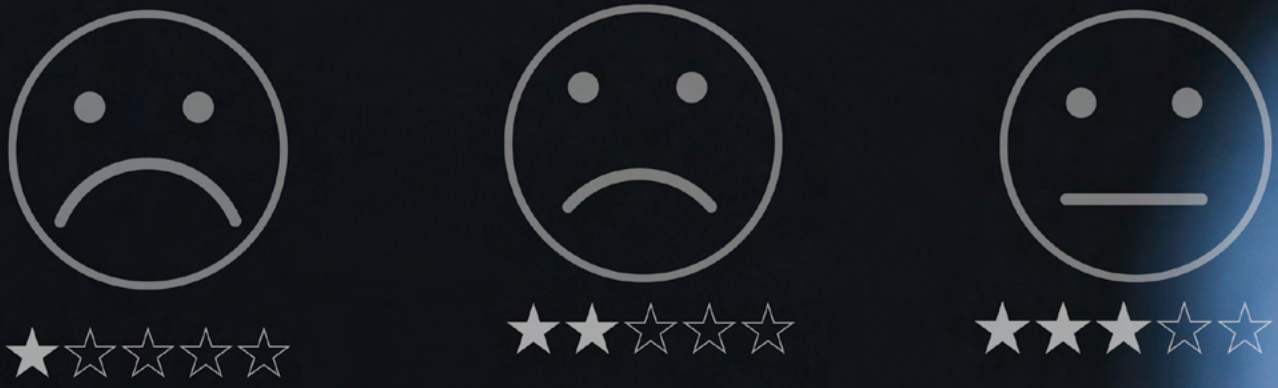
CDO
Mauro Nunes

CX Regional Manager
Nadia Simón

HR Manager
Verónica Funes

Strategic Communications Director
Flor Palazzolo

SUMARIO



CX Files

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

La experiencia del usuario es uno de los factores clave del éxito de una organización. En este artículo descubrirás cuáles son los principales puntos a tener en cuenta para desarrollar una estrategia enfocada en la satisfacción del cliente.

Todo,
en todas partes y al mismo tiempo

El título de la película ganadora del Oscar es una síntesis de lo que se debería esperar de las áreas de Customer Success (o Customer Experience). La realidad nos muestra que estamos lejos de eso. Veamos un par de ejemplos.

Son momentos de aceleración en el despliegue de las prácticas de CX/CS en organizaciones de todo el mundo. El tema aparece en la agenda de todas las reuniones, y las preguntas más comunes son similares entre los líderes: ¿Cómo hacer? ¿Dónde obtener buenos CSMs (Customer Success Managers)? ¿Qué herramienta usar, un desarrollo propio o adquirido? ¿Cuánto invertir en relación al revenue recurrente? ¿Cómo mejorar la tasa de renovaciones?, y similares.

Las dudas también son comunes: ¿Realmente vale la pena? ¿Sirve para organizaciones medianas? ¿A los clientes les resulta relevante?, y otras similares. En el fondo de todo esto quedan las 2 preguntas clave que habitualmente no se realizan, o cuya respuesta se esquiva:

1.- ¿Cuál es el modelo de negocio del área de CX/CS?

Sin un modelo de negocio no hay práctica válida de CX, y esto implica tocar todos los ángulos: empezando por la contribución a los flujos de dinero, la inversión necesaria, las cuentas foco, el equipo y su interacción con todas las áreas, el impacto en el resto de los roles y la comunicación interna y externa.

Uno de los errores más comunes es asumir que CX es un apéndice de otra área. Ese error se transforma en horror cuando se la adjunta a Ventas, con lo que en la mayoría de las veces se embarran los beneficios y se termina desvirtuando su función. Los resultados son menos malos cuando se la adjunta a Servicios, pero sólo si se respetan los objetivos de centrarse en el éxito del cliente y no en el propio. Lo que nos lleva al próximo punto.

2.- ¿Cuáles son las métricas?

El latido del modelo de negocio lo dan las métricas que se elijan. La creación de un área de CX debe, por fuerza, tener medidas y dinámicas propias pero que impactan en todas las demás: Ventas tiene interacciones enriquecidas con los clientes; Finanzas tiene una visión íntima y anticipatoria de porqué un cliente tiene propensión, o no, a continuar siéndolo; Servicios se puede concentrar en lo transaccional pero con mucha mejor noción del sentimiento del cliente.

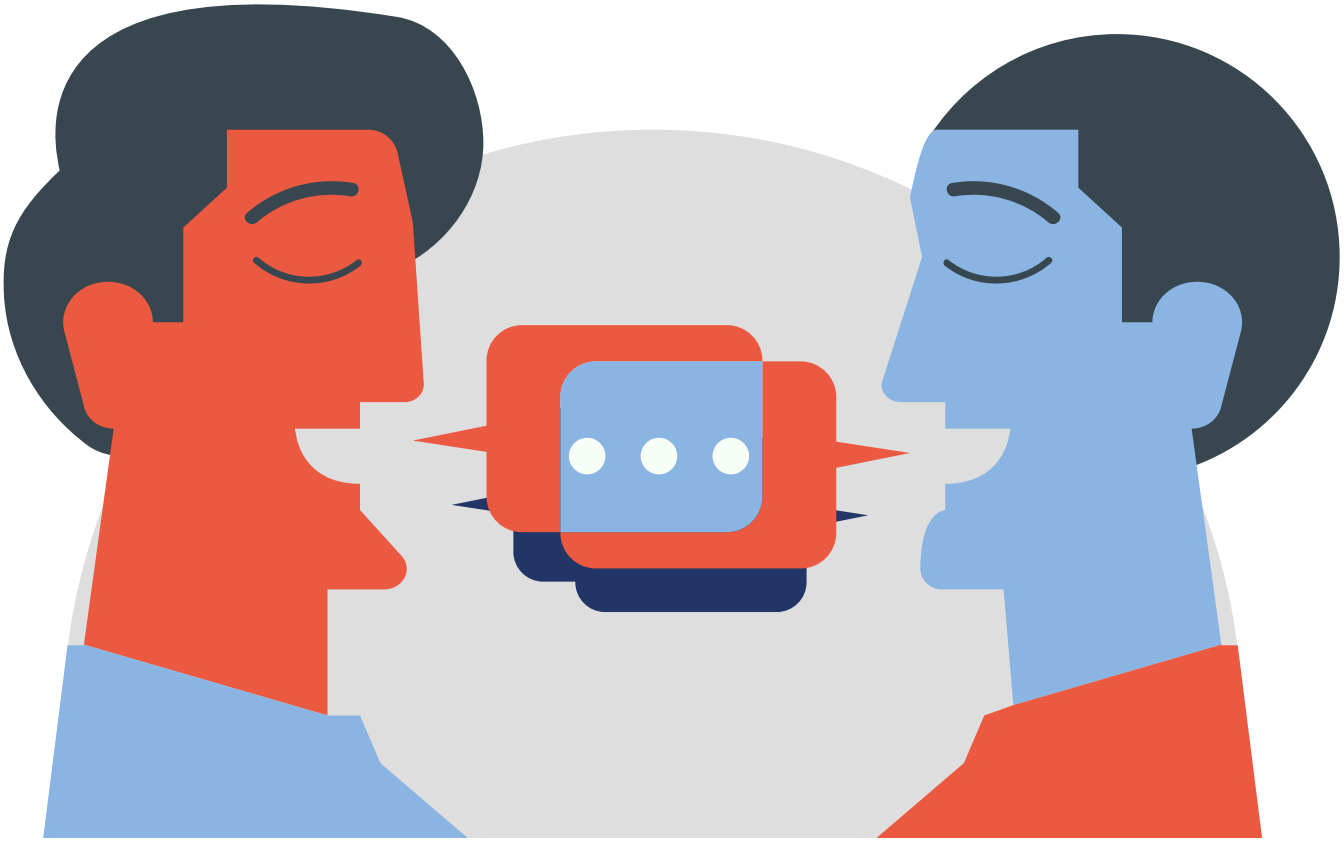
La métrica fundamental del área de CX es el éxito de los usuarios, medido en las métricas de ellos mismos (los usuarios). Ninguna otra es más importante. Claro, eso impacta en el NPS (Net Promoter Score), en la tasa de renovaciones, en la fidelidad, etc.; todas ellas, métricas del proveedor.

El éxito del cliente debe ser el foco único y la razón de ser. De allí surgen nuevas formas de trabajo interno, afectación a los modelos de compensación, cambios en las dinámicas de comunicación y reformulación de las métricas fundamentales de la organización.

La llegada de CX cambia todo, y afecta al conjunto de las dinámicas organizacionales tradicionales.

Todo, en todas partes, y al mismo tiempo.
De eso se trata.

El ser humano y su VOZ para mejorar la experiencia del cliente



El cliente y su experiencia es el corazón para toda organización. Hoy, las empresas no sólo ofrecen productos o servicios, sino valor agregado, una experiencia. Cada punto de contacto con los clientes puede mejorar o perjudicar la percepción que tienen de la marca. Poner al cliente en el centro de la estrategia significa abordar esta transformación que incluye acciones y emociones, explorar nuevas aristas, innovar y evolucionar, observar los distintos condimentos que impactan, irrumpen, reinventan la forma de hacer negocios. Uno de ellos es la comunicación empática, que cobra cuerpo -por ejemplo- a través de la voz de los empresarios y sus colaboradores.

"Cuando hablamos de la experiencia del cliente, entra en juego lo vivencial, el acercamiento, la confianza…", dice Nadia Simón, CX Regional Manager en OCP TECH, y agrega que actualmente coexisten factores que, hasta hace algunos años, no se hubiesen considerado a la hora de montar negocios.

¿Cómo transmitir correctamente? ¿Qué rol tiene la voz en esta tarea? Este tema es el origen del conversatorio encabezado por **Nadia Simón**, y que suma el valioso aporte de **Pablo Marrone**, consultor en Customer Experience, y **Claudia Menkarsky**, Vocal Coach.

Mira el conversatorio en vivo

La **voz** de las empresas

Pablo Marrone opina que “hoy los clientes buscan sentir que están siendo escuchados en su necesidad y que los van a acompañar a lo largo del camino”. Coinciden en que está cambiando la forma de hacer negocios: “Hoy muchas empresas ofrecen productos o servicios parecidos, el cliente busca el diferencial. Es más o menos lo que pasa cuando vamos a un restaurante. ¿Volvemos por la comida? No, volvemos donde vivimos la mejor experiencia. Y en esta experiencia del cliente incide la atención del mozo, la confianza que nos inspira, su actitud, su manera de comunicarse”.

Para Claudia Menkarsky, “nuestra voz nos identifica y nos define”. Opina que, para sentirse bien con la propia voz, es preciso observar la gestión emocional, manejar los tonos, el ritmo, la frecuencia, la velocidad, la empatía. Entonces, es posible comunicarse plenamente, marcar la gran diferencia.

El camino para gestionar adecuadamente la voz y la forma de comunicarse comienza cuando se toma conciencia de la propia respiración: “La voz fluye con nuestro aliento y transmite el estado de conciencia, las emociones, nuestra energía. A partir del autoconocimiento, nos transformamos para transmitir aquello que queremos, de la forma adecuada”. A partir de su *expertise* como Vocal Coach, destaca la oportunidad de respirar profundo para volver a conectarnos: “La respiración regula el sistema nervioso, nuestro pulso cardíaco y hace que nos centremos. Respirando profundo nos oxigenamos y siempre vamos a encontrar en esa inspiración, en esa conexión interna, un eje para regular las emociones y poder hablar desde lo mejor de nosotros mismos”.

Profundiza: “Del silencio nacen todas las palabras. Entonces la escucha es la primera instancia a partir de la cual vamos a poder tener ese tiempo de reflexión para encontrar aquellas palabras apropiadas, en base a lo que vemos y deseamos comunicar y transmitir”. Cada ser humano tiene su forma de hablar: “Cada voz es única y cada vez que hablamos estamos transmitiendo de una forma muy particular y definida nuestro ser en esa voz”. Dice que encontrar la propia voz tiene nexo con ese infinito que somos, que es individual y que también depende de la energía y del encuentro con el otro.

Claudia Menkarsky agrega: “Cada voz tiene su luz y aquello que damos es único, es una mirada de este multiverso personal que llega con la propia frecuencia y energía. Es fundamental que cada uno encuentre su luz, su voz, su conciencia, para poder comunicarse de la mejor forma”.

Pasión por el trabajo

Una vez que encontramos la propia voz que nos define: ¿Cuál es el secreto para la comunicación eficaz? “Estar convencidos de aquello que queremos dar, hablar apasionadamente. A partir de ahí, vamos a poder transmitir de la mejor manera”, dice Menkarsky. Desde la óptica de Simón, entran en juego distintas variables, como la relación interpersonal, comprender el objetivo y la misión, saber dónde estamos y hacia dónde vamos: “En nuestro caso, el esquema organizacional es abierto y transparente. Impulsamos la amabilidad para dirigirnos, por ejemplo, a un compañero que no puede acceder a una conexión o que tiene un problema con una herramienta de trabajo… es tan simple como acercarse y ofrecer ayuda. Esto es Customer Experience también”, agrega.

Para Pablo Marrone, la satisfacción del cliente es la filosofía que envuelve a la organización: “Hace un tiempo hablábamos de Calidad Total, un concepto que tocaba todo. Esto es lo mismo, involucra a todas las áreas”. Añade: “Muchas veces, cuando se hace una consultoría en Customer Success, lo primero que uno ve es la resistencia al cambio. Tenemos que estar dispuestos a cambiar. Y también ser empáticos, tener noción de ese otro. Customer Success existe porque hay una persona del otro lado del mostrador, en cualquiera de sus roles. En nuestra actividad, muchas veces tendemos a centrarnos en lo tecnológico y nos olvidamos de esa empatía, esa necesidad de comunicarnos con el otro”.

Nadia Simón y Pablo Marrone coinciden en que actualmente las organizaciones reconocen que toda la estructura está atravesada por gestionar la mejor experiencia del cliente. Cada empleado, cada área de la empresa es responsable de una parte de esa experiencia.

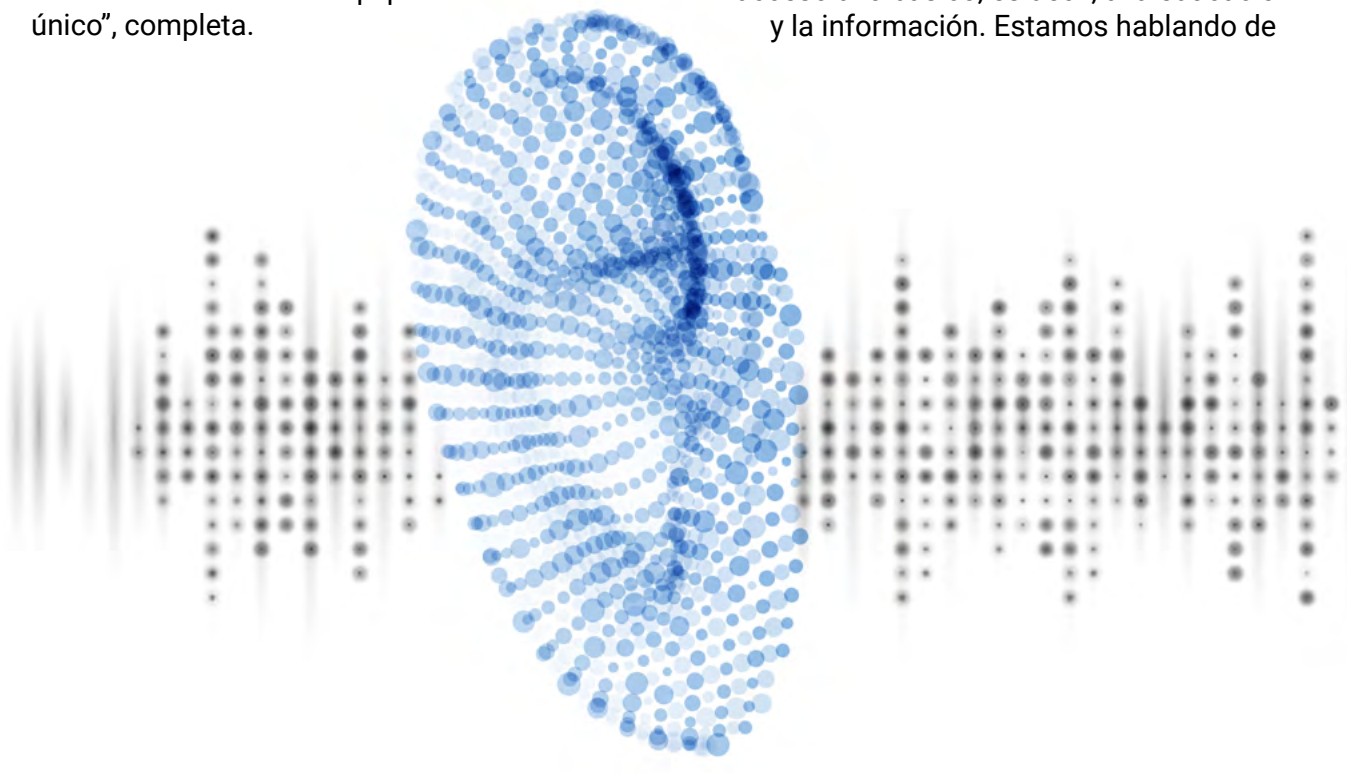
En OCP TECH, “la operación es transversal al esquema del cliente y todas las áreas se retroalimentan. Nuestro símbolo es el infinito que tiene que ver con el seguimiento continuo. Desde hace varios años, impulsamos esta cultura”, indica Nadia Simón. En el equipo conviven distintos perfiles que funcionan como un todo: “Es nuestro diferencial. A la hora de abordar la experiencia del cliente, funcionamos como un equipo único”, completa.

Moda o una realidad en evolución

“Desde el punto de vista organizacional, creo que estamos presenciando algo que dista mucho de ser una moda. Mi opinión es que el Customer Success o el Customer Oriented Executive va a ir escalando, hasta liderar los equipos integrados por Ventas, Producto, Estrategia, Marketing”, augura Pablo Marrone.

Claudia Menkarsky aporta que, en medio de la tecnología, la humanización es inminente: “Viene un renacimiento de lo humano, donde la tecnología va a cobrar vida y vuelo, no ya como un simple medio, sino con la trascendencia de poder transmitir valores e información tan necesaria para todos. Cuando está al servicio del ser humano, es maravillosa porque llega a todas partes”.

Nadia Simón subraya que una vez que se ingresa en el Customer Experience es imposible tener otro abordaje con el cliente: “Tengo más de 25 años en el mercado, y hoy creo que se pueden generar vínculos desde otro lugar. Es posible aportar valor y cambiar. Nuestro trabajo tiene un impacto social. A diario vemos cómo chicos que están en lugares distantes acceden a la comunicación… se enciende esa conectividad y comprendemos que estamos cambiando la vida a una persona, dándole acceso a lo básico, es decir, a la educación y la información. Estamos hablando de



Nadia Simón
CX Regional Manager
en OCP TECH

Claudia Menkarsky
Vocal Coach

Pablo Marrone
Consultor en Customer Experience

tecnología, pero a nivel social tiene un gran impacto, y eso es el diferencial, lo que te hace levantar todos los días y decir ´bueno, vamos a hacer que las cosas pasen´. Desde mi posición y desde la compañía, realmente, hacemos que las cosas sucedan, junto al equipo, que tiene un gran compromiso".

El método es construir el mejor vínculo con todos los actores, indagar sobre las mejores formas de expresar y comunicar, reconocer y gestionar la propia voz, hacer pausas para reorganizar, escuchar, comprender y así establecer el mejor diálogo.

Achicar la brecha

El desafío de OCP TECH es mejorar las comunicaciones, integrar los distintos perfiles -tanto jóvenes como experimentados-, y estar a la altura de las tendencias y demandas: "Estamos alineados en esta tarea", dice Nadia Simón, y pone el foco en la necesidad de, además de aprender a comunicar, saber escuchar, siempre en sintonía con las distintas audiencias.

Claudia Menkarsky aporta: "Es muy interesante lo que dice Nadia, ya que hoy hay una brecha generacional lingüística enorme, no es lo mismo cómo le vamos a hablar a una persona de cuarenta años o a alguien de veinticinco. El tema del lenguaje juega un papel fundamental. Transmitir con un lenguaje claro es clave para una buena comunicación en toda empresa".

Metaverso

META (más allá)
VERSO (universo)

La palabra “metaverso” es un acrónimo compuesto por ‘meta’, que proviene del griego y significa “después” o “más allá”, mientras que ‘verso’ hace referencia a “universo”. Se trata de un ecosistema virtual y tridimensional (3D) en el que los usuarios pueden interactuar entre ellos, trabajar, jugar, estudiar, realizar transacciones económicas, entre muchas otras posibilidades. Todo ello de forma descentralizada.

¿Qué lo hace posible?

Tecnologías como el *blockchain*, la realidad aumentada, la realidad virtual, 3D, la inteligencia artificial o el internet de las cosas.

¿Cómo se participa?

El ingreso a este espacio se realiza a través de nuevas interfaces como las gafas inteligentes o los guantes hápticos, que nos permiten explotar las capacidades de inmersión de forma sensitiva. Además, las tecnologías de *blockchain* y NFT (token no fungible, por sus siglas en inglés), introducen unidades de valor que se pueden intercambiar en forma de compra y venta.

El desafío

Pasar de los metaversos -en plural, al metaverso -en singular. Hoy no existe un único metaverso pues las distintas propuestas son independientes y no están conectadas entre sí, se comportan como silos cerrados y los elementos o experiencias de una plataforma aún no pueden utilizarse en otras.

Principales retos para lograr este objetivo

- Alcanzar la interoperabilidad entre los distintos universos o plataformas a fin de poder utilizar avatares, monedas y experiencias en los distintos entornos. En este sentido, la tecnología *blockchain* puede contribuir pues da la capacidad de poseer valor y transferirlo sin necesidad de un tercero.
- Construir espacios altamente seguros que protejan los datos personales y las transacciones.
- Preservar la ética de los actores del espacio virtual a la vez que se construyen experiencias y actividades con responsabilidad.
- Abordar asuntos legales que contemplen cuestiones tales como si tendremos las mismas obligaciones y derechos que en el mundo real o si se aplicarán las mismas leyes que en el físico.
- Contemplar el desafío psicológico que este entorno en 3D plantea para las personas que experimenten en él.
- Para las marcas se podría convertir en una nueva forma de interactuar con los consumidores, a través de distintas experiencias inmersivas y la generación de una comunidad con valores afines que facilite volver al entorno.


Web 1.0
Hipertexto: *links* o enlaces.
Web 2.0
Interacción: redes sociales.
Experiencias en dos dimensiones.
Web 3.0
Creación e intercambio de activos digitales
-NFTs- utilizando la tecnología *blockchain*.
Experiencias en tres dimensiones.

Datos curiosos

- La palabra metaverso tiene 31 años y fue creada por Neal Stephenson en su novela de ciencia ficción de 1992 Snow Crash, que prevé un sucesor de Internet basado en la realidad virtual.

- *Metaverse Market* alcanzará los US$ 936.6 mil millones para 2030 a una CAGR (tasa de crecimiento anual compuesta) de 41.6% - *Grand View Research, Inc.*

- Uno de los primeros acercamientos de la ley a este nuevo universo tuvo lugar en Nueva York, cuando la Justicia falló a favor de la compañía *MetaBirkin*, que había alegado la infracción de los derechos de su marca registrada. En la causa, la empresa declaró que se estaban vendiendo bolsos virtuales del modelo "Birkin" en formato NFT.

5 películas para entender el metaverso

Free Guy (2021) - EE.UU.
Dirección: Shawn Levy

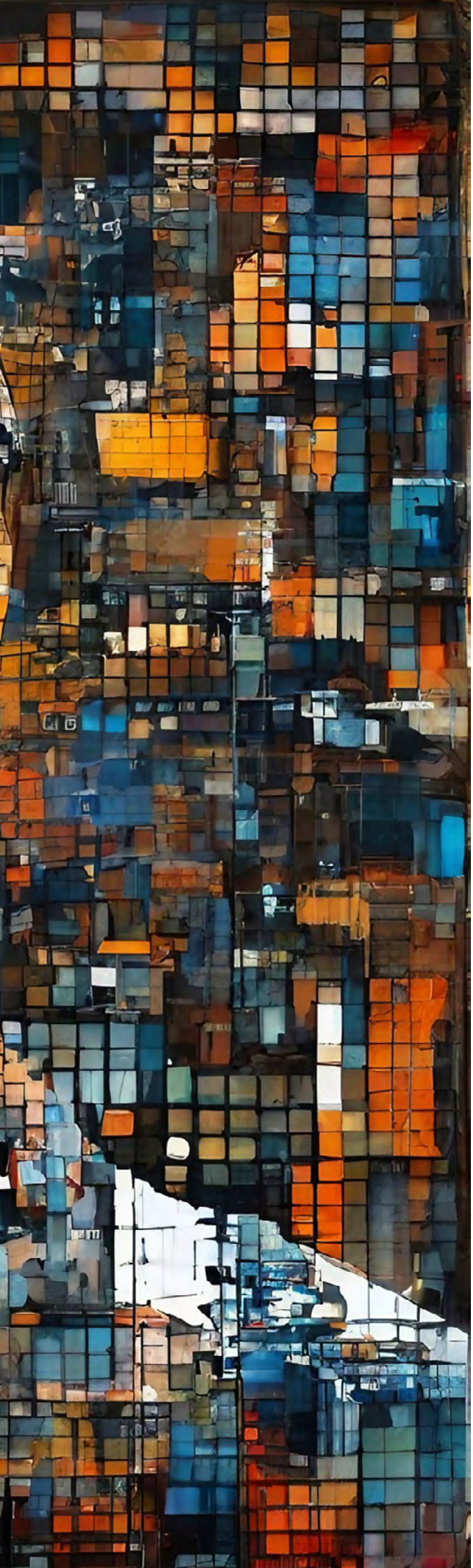
Ready Player One (2018) - EE.UU.
Dirección: Steven Spielberg

Desafío total /El vengador del futuro (1990) - EE.UU.
Dirección: Paul Verhoeven

Snow Crash (2014) - EE.UU.
Dirección: Joe Cornish

Existenz (1999) - Canadá
Dirección: David Cronenberg

La posibilidad de conservar una misma identidad en los diversos universos paralelos no será solamente un deseo de orden estético. La interoperabilidad es deseable en más sentidos, por ejemplo, para poder usar los elementos que se hayan adquirido en diferentes ámbitos, para acreditar nuestra identidad y comportamiento, para conservar nuestro historial, tal como sucede en el mundo físico.



Arte by IA

La inteligencia artificial generativa está pisando fuerte. Con uso responsable y adecuándola al contexto necesario, puede ser de ayuda o complemento de nuestro saber.

Le pedimos a *Clipdrop, by stability.ai* que genere para nosotros una obra digital que ilustre al hombre inmerso en sus pensamientos futuros y sin embargo, establecido, anclado, en pertenencia con su ciudad.

Este es el resultado. ¿Qué te parece?

Entrevista

Leonardo Scatturice

Founder and CEO, OCP TECH

por **Flor Palazzolo**

Flor: Leonardo, gracias por tomarte tu tiempo para participar de esta primera edición de nuestro anuario. De alguna manera estamos de festejo, ¿no? *Risas*.
Para comenzar esta entrevista, me gustaría que compartieras un poco sobre ti mismo. ¿Qué puede decir Leonardo de Leonardo?

Leonardo: ¡Qué comienzo, Flor! Es verdad, estamos de festejo. Este anuario es un puntapié perfecto para conectarnos y dar a conocer la esencia de OCP TECH. Acercándome a tu pregunta, creo que es ciertamente complejo hablar sobre mí mismo. Hace años quizás te respondía con calificativos y grandes palabras pero, ya con cierta experiencia te diría que esa respuesta se encuentra al tomar retrospectiva respecto a mis acciones. Algo que me caracterizó a lo largo de los años fue la necesidad constante de abrir nuevos caminos y fortalecer mi visión del futuro. En definitiva, creo que cada ser humano busca potenciarse y sentirse parte de

Leonardo Scatturice en la oficina central de OCP TECH, Miami, FL.

algo mayor, y así, de alguna forma, impactar en la realidad y dejar huella. Siempre he creído en la capacidad de la tecnología para transformar vidas y mejorar empresas… de alguna manera la existencia de OCP TECH y su constante expansión es una huella que habla mejor de mí que cualquier otra cosa. Fundar esta empresa habla de un Leonardo que busca impulsar a un equipo para marcar una diferencia, y eso es algo en donde sí me veo, te diría que el trabajo en equipo fue uno de los factores claves tanto en mi construcción personal como profesional.

Flor: Respecto a esto último que mencionas, desde luego eres ampliamente reconocido como un líder visionario, pero ambos sabemos que esta responsabilidad conlleva desafíos. ¿Existe algún contrapeso en tu rol de líder? ¿Cuál?

Leonardo: Claro, Flor. Ser un líder visionario es emocionante, pero también es un desafío. Creo que un contrapeso importante es mantener un equilibrio entre la innovación y la estabilidad. Siempre estamos buscando nuevas formas de crecer, porque eso representa la esencia misma de la empresa pero también debemos asegurarnos que nuestra base esté sólida y que nuestros equipos estén alineados con nuestra visión.

“Somos impulsores del cambio y creemos en hacer una diferencia positiva en la vida de las personas”.

Flor: Hablando de eso… Tu visión para OCP TECH fue expansiva, la empresa ha desarrollado una gran presencia en varios países de Latinoamérica. ¿Cuál es el principal desafío que plantea esta apertura?

Leonardo: La expansión a Latinoamérica ha sido un hito emocionante para todo OCP TECH. El principal desafío radica en comprender y adaptarnos a las diferentes culturas y mercados en la región. Cada país tiene sus propias necesidades y desafíos, y debemos ser flexibles y ágiles para brindar soluciones que se ajusten a estas particularidades. Ha sido un trayecto arduo, en donde muchas personas trabajaron muy duro y todavía falta más… Creo que vamos por buen camino, al cierre de esta edición ya tenemos presencia en 15 países, sin embargo nuestra visión de compañía no se conforma con eso, así que continuaremos el rumbo expansivo.

Flor: Desde luego que sí. Ahora, me permito entrar en sentidos que algunos llamarían metafísicos… háblame un poco sobre el alma de OCP TECH. ¿Cómo describirías la esencia de la empresa?

Leonardo: El alma de OCP TECH es la ingeniería de impacto, a través de la innovación constante y el conocimiento. Somos un equipo apasionado y enfocado en buscar soluciones tecnológicas avanzadas para nuestros clientes. Nuestra esencia radica en la creatividad, la colaboración y el compromiso con la excelencia. Somos impulsores del cambio y creemos en hacer una diferencia positiva en la vida de las personas.

Flor: Eso suena verdaderamente inspirador. Ahora pensando en lo material ¿Cómo es el cuerpo de OCP TECH?

Leonardo: Desde luego que el cuerpo de OCP TECH son nuestros empleados, clientes y socios. Somos un equipo global, diverso y altamente capacitado que trabaja en conjunto para ofrecer soluciones integrales. Nuestros clientes y socios son la base de nuestro crecimiento y éxito. Son

Andrés Quinn, *COO de OCP TECH y*
Leonardo Scatturice, *CEO, en diálogo constante acerca de cómo acercar la innovación a sus clientes.*

parte fundamental de nuestro cuerpo, y siempre estamos buscando maneras de fortalecer estas relaciones a largo plazo.

Flor: Uno de nuestros sentidos transversales en OCP TECH refiere a ser una organización Customer Centric. ¿Qué significa este concepto para tí?

Leonardo: Ser una organización Customer Centric es esencial para nosotros. Significa que estamos orientados a nuestros clientes en cada paso. Escuchamos atentamente sus necesidades, deseos y desafíos, y creamos soluciones que los beneficien. Nuestro enfoque está en construir relaciones a largo plazo, brindarles un servicio excepcional y superar sus expectativas. Hoy en día, en un mercado tan competitivo la mejor estrategia es volver a la necesidad del cliente, a su realidad.
En definitiva, el mayor valor agregado que puede otorgar nuestro servicio es la noción de que está pensado directamente desde sus necesidades reales. Nos enfocamos en sus requerimientos de negocio, proponemos soluciones tecnológicas en forma proactiva y a través de una madura práctica de CX, los acompañamos en el ciclo completo del uso eficiente de la tecnología.

Flor: Para concluir y de alguna manera volviendo al inicio, donde compartiste con nosotros tu necesidad de construir hacia el futuro ¿hacia dónde miran hoy los ojos del Leonardo emprendedor?

Leonardo: Los ojos del Leonardo emprendedor siguen mirando hacia el futuro con gran entusiasmo y determinación. Nuestro enfoque está en la expansión continua, la innovación constante y en llevar a OCP TECH a nuevos horizontes. En el mundo actual, estos nuevos horizontes nos tienen que encontrar más conectados que nunca, buscando retroalimentación de nuevas experiencias, ideas y tecnologías. La verdad Flor, es que estoy emocionado por lo que el futuro nos depara y confío en que juntos lograremos seguir generando el impacto significativo que el universo de la tecnología necesita.


OCP
TECH
global IT

Fraude y Ciberseguridad

Existen escenarios donde los intereses de áreas como ciberseguridad y prevención de fraudes sufren divergencias, consecuencia de sus necesidades específicas y búsqueda de resoluciones rápidas, las cuales no necesariamente son las más adecuadas de cara a la protección de datos personales o sensibles. ¿Es posible lograr el equilibrio entre los requerimientos y necesidades de Prevención de Fraude y los de Ciberseguridad? ***Fabio Sánchez****, Director de Prácticas de Ciberseguridad, OCP TECH y* ***Eric Balderrama****, Abogado, Co Founder de Trully, abordan la cuestión desde distintos puntos de vista, como ser el del emisor del medio de pago, el comercio y el usuario final, a la vez que aportan algunas ideas para optimizar los procesos de estas áreas. Aquí algunos textuales de la conversación.*

Contexto

Nuestro entorno actual tiende hacia la digitalización y el ambiente no presente en términos transaccionales. Esto provoca que los equipos de Prevención de Fraude necesiten verificar la identidad de los usuarios de maneras alternativas a la tradicional, donde el usuario se presentaba de manera física a aperturar una cuenta o transaccionar. Es común encontrar organizaciones que ya han implementado mecanismos de autenticación biométrica para el proceso de apertura de una cuenta y de MFA (Autenticación Multifactor, por su sigla en inglés) para transaccionar, como ser un *token mobile* o un sms con un

código

Mira el
resumen aquí.

OTP (del inglés One Time Password).
Sin embargo, hay escenarios donde los delincuentes logran eludir o manipular estos procesos digitales realizando acciones fraudulentas como suplantación de identidad, robo de cuentas o abuso de la lógica de negocio por mencionar algunos.

Fabio Sánchez afirma, "Desde ciberseguridad, la prioridad es proteger la confidencialidad, integridad y disponibilidad de la información que se está tratando. La recomendación para usuarios finales, suele ser que evite brindar información personal relacionada a nombre, tarjetas de crédito, dirección, etc., a fin de minimizar la posibilidad de que sea utilizada en fraudes, sin embargo, esto dificulta enormemente la usabilidad, practicidad y simpleza a la hora de operar. Encontrar el equilibrio entre seguridad y usabilidad es uno de los problemas más grandes: cuándo sí y cuándo no brindar esa información, qué dar y cuándo hacerlo".

"Creo que la problemática está un nivel más arriba. En líneas generales, la mayoría de los equipos de ciberseguridad y de fraude no se alinean, no se hablan, sí pertenecen a una misma compañía pero trabajan en silos: Ciberseguridad de cara a cubrir los cumplimientos regulatorios asociados a su área y Prevención de Fraude, buscando el equilibrio entre prevenir fraudes y prevenir ventas. ¿Por qué? Porque en lugar de ser *frictionless* para la persona que quiere hacer una compra o una transacción, se le empiezan a poner barreras o controles adicionales para protegerlo, que, en muchos casos terminan evitando la venta. El entorno actual habla de falta de comunicación y falta de definición de estándares y lineamientos entre ambas áreas", responde ***Eric Balderrama***.

"En un contexto donde todo tiende a autenticarse de manera remota es mucho más complejo poder identificar quién es quién desde el área de Prevención de Fraude. ¿Qué elementos tenemos para validar que Fabio es Fabio? Usualmente se utiliza identificación y *selfie*. Para hacer esa validación existen algunos sistemas que operan durante el proceso de originación conocidos como KYC (del inglés Know Your Curstomer), sin embargo esto no es suficiente, dado que si bien regulatoriamente puede ser *compliance*, no necesariamente es una barrera efectiva para combatir el fraude. Posteriormente, cuando el cliente empieza a transaccionar, ¿cómo validar que Fabio es realmente Fabio? Hay diferentes metodologías, por ejemplo el análisis conductual es uno: si Fabio compra en cuatro o cinco *e-commerce* y de repente vemos una transacción en otro lado con un costo muy alto, está bien frenarlo y pedir un segundo factor de autenticación, que no necesariamente tiene que ser que la persona mande una foto de su tarjeta y una suya, aquí es donde el proceso de Prevención de Fraudes entra en conflicto con Ciberseguridad, por la protección de la información. Este es un punto clave donde se evidencia la falta comunicación entre Ciberseguridad, Prevención de Fraude y también AML o Cumplimiento".
Eric Balderrama.

"Los objetivos de ambas áreas son distintos. Uno, desde el punto de vista del negocio es evitar el fraude, robo o suplantación de identidad y no afectar la venta. El de ciberseguridad es el de resguardar la información mediante la aplicación de controles y capas de seguridad, que posiblemente, van a dificultar y poner más trabas a los proceso de originación y transacción". ***Fabio Sánchez***.

"También hay que entender cuáles son las prácticas, lo que ya está implementado y asimilado. La mayoría de leyes de protección de datos personales de los países están basados en la CEPAL (Comisión Económica para América Latina y el Caribe) donde establecieron una ley modelo de datos personales. No significa que una empresa esté legalmente restringida a pedirte una foto de tu tarjeta o tu documento, pueden hacerlo, pero para eso lo ideal es que tengan un aviso de privacidad público y allí mencionen los tipos de datos sensibles que van a estar solicitando, cuál va ser el tratamiento que le van a dar y durante qué período de tiempo va a estar almacenada esa información. Por ejemplo, algunas plataformas de venta digital de pasajes no tienen estos procesos, te piden 'mándame la foto de tu documento y de tu tarjeta de crédito para poder validarte', eso se puede denunciar. En cada uno de los países hay distintos canales para hacerlo: en el caso de Argentina está Consumo Protegido, en el caso de México está PROFECO (Procuraduría Federal del Consumidor). El usuario debería

ejercer su derecho para poder empujar a que estas compañías se adecúen a la normativa. Por otro lado y entendiendo a los equipos de fraude, hay una explicación de por qué hacen eso: es una práctica que ya está implementada. Imaginemos brevemente ser parte de un equipo de Prevención de Fraudes ¿cómo valido que una persona es realmente quien está queriendo realizar una transacción? ¿Cómo lo hago de forma fácil, rápida y simple? A estas preguntas, luego deberíamos sumarle ¿Es la manera correcta? ¿Hay maneras más correctas?". *Eric Balderrama*.

Responsabilidades

Medio de pago emisor

Actualizar su tecnología a fin de contar con soluciones que faciliten tanto la tarea del comercializador como del usuario final.

Comercio

Contar con tecnología de doble factor de autenticación.
Promover políticas de protección de datos personales.
Actualizar sus sistemas internos.
Alinear las áreas de Ciberseguridad y Prevención de Fraude, promover su comunicación y equilibrar sus objetivos.

Usuario

Resguardar su información personal y ser cuidadoso al brindarla.

"Al implementar métodos alternativos de verificación y de conocimiento del cliente, para verificar que es quien dice ser, no tengo que estar, como empresa, pidiéndole más información de la que necesito. Y tampoco voy a tener que estar guardando la información y preocupándome dónde la guardé, cómo la voy a proteger. Al aplicar métodos alternativos para verificar la autenticidad de la persona, creo que le facilitamos la vida al usuario y hacemos más grata su experiencia de compra". *Fabio Sánchez*.

"A nivel de empresas también es importante implementar un buen sistema de gobierno de datos. Porque luego pasa lo que dice Fabio, existe información asociada a un usuario dispersa en diferentes lugares, en bases de datos, directorios compartidos, en la computadora de un colaborador, y cuando un usuario haga uso de sus derechos, por ejemplo a través de Derechos ARCO (Acceso, Rectificación, Cancelación y Oposición), la empresa va a borrar solamente los datos que tiene registrados en la base de datos, sin embargo en los demás espacios seguirá disponible. Esto va contra la protección de datos personales del titular". *Eric Balderrama*.

Soluciones tecnológicas posibles

OTP (One time password), por ejemplo 3DS (Secure): Según el monto de la transacción, se envía un *token* por teléfono al comprador, éste introduce el OTP en el flujo transaccional y ¡listo!

CVV dinámico: En escenarios de tarjetas digitales, los tres dígitos de validación de la tarjeta de crédito VISA o Mastercard, o cuatro dígitos en el caso de AMEX, van cambiando con un tiempo definido. Esto hace que el CVV termine funcionando como un OTP.

Chip + PIN: Para canales presenciales con tarjeta física. El PIN actúa como segundo factor de autenticación, dado que confluye algo que tengo (Tarjeta) con algo que sé (PIN).

Validación mediante un pequeño monto transaccionado: Solamente el usuario va a tener acceso a su cuenta para poder identificar el monto exacto de la transacción. "Yo lo he implementado y el costo es muy bajo. Es una excelente alternativa. Algo muy bueno que puede salir de esta conversación es sensibilizar con respecto a esta solución. En lugar de pedir al usuario el documento y la tarjeta de crédito, mandar un cargo pequeño de menos de un par de centavos a la tarjeta de crédito del usuario, él dice de cuánto fue y de esa manera se valida". *Eric Balderrama*.

Recomendaciones

Empresas

Aplicar seguridad en profundidad a nivel de prevención de fraude. Tener KYC (Know Your Customer) pero robustecer el proceso de originación con datos alternativos y de ser posible apoyarse en redes colectivas de prevención de fraudes. Fortalecer el proceso

transaccional del usuario con OTPs, *tokens*, etc., para autenticar y validar operaciones.

Entender cómo se comporta el comprador. Si siempre utiliza determinadas tarjetas de crédito y cierto día presenta un cambio de medio de pago, validar con él si realmente hizo la transacción.

Alinear la comunicación entre Ciberseguridad y Prevención de Fraude para implementar controles que le faciliten la vida a los usuarios, resguardando la información.

Implementar métodos alternativos que eviten solicitar información personal, avalados por tecnologías disponibles y que facilitan el proceso.

Usuarios

Tomar responsabilidad sobre sus datos personales.

Invertir tiempo para revisar los resúmenes de cuenta de las distintas tarjetas.

Leer los avisos de privacidad, términos y condiciones de las plataformas o sus síntesis vía algún servicio GPT: ver qué datos cedemos, para qué los van a utilizar y cuál es la política y período de retención. También si está contemplada alguna forma de que se eliminen.

Tomar medidas de seguridad aplicando segundos factores de autenticación.

Tomar control de los accesos y verificarlos.

Ser celosos con la información que compartimos y evitar naturalizar el proceso de cederla.

De qué hablamos cuando hablamos de Datos Personales

Existen regulaciones regionales en varios países. En LATAM existe también la Ley Modelo de Protección de Datos Personales de la Comisión Económica para América Latina y el Caribe (CEPAL), que es una guía y referencia para los países de la región en el desarrollo de sus leyes nacionales de protección de datos. Aunque la Ley Modelo no es vinculante por sí misma, ha sido utilizada como base para la creación o revisión de las legislaciones de protección de datos en varios países latinoamericanos.

En cada país la definición de "dato personal" puede presentar algunas particularidades, sin embargo, en general son:

Datos de identificación: Nombre, apellido, número de identificación (como el número de cédula o pasaporte), fecha de nacimiento, género, nacionalidad, entre otros.

Datos de contacto: Dirección de domicilio, número de teléfono, dirección de correo electrónico u otra información de contacto personal.

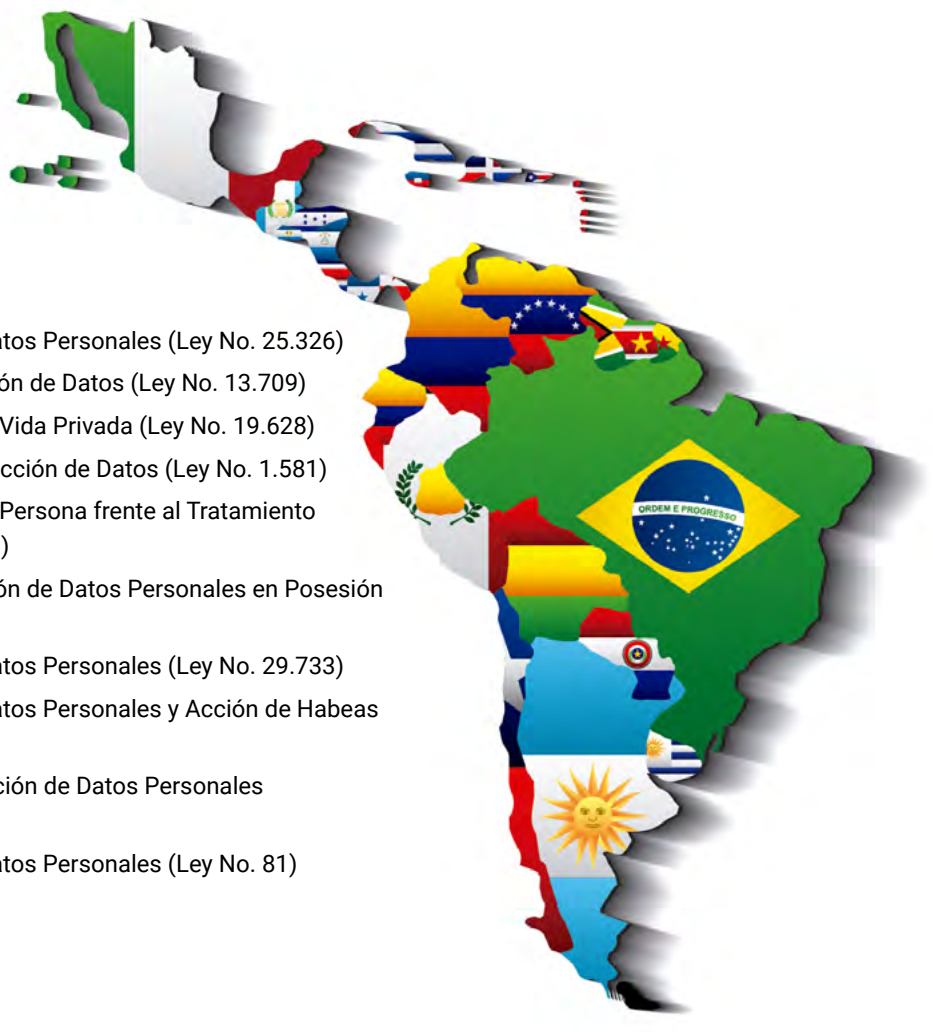
Datos sensibles: Información relacionada con la salud, origen racial o étnico, creencias religiosas o filosóficas, afiliación sindical, orientación sexual, antecedentes penales, entre otros.

Datos financieros: Número de cuenta bancaria, tarjetas de crédito o débito, historial de transacciones financieras, ingresos, deudas, entre otros.

A fin de operar de forma eficiente en las distintas organizaciones, los equipos de las áreas de Legales, Ciberseguridad y Prevención de Fraude tienen la responsabilidad de interiorizarse y revisar la legislación que aplica en cada país y cómo se expresa respecto a los datos personales, incluyendo el consentimiento informado, la finalidad legítima, la calidad de los datos, la seguridad de la información y sus responsables durante el procesamiento, resguardo, transmisión y destrucción.

Legislación por país en Latinoamérica

País	Ley o regulación
Argentina	Ley de Protección de Datos Personales (Ley No. 25.326)
Brasil	Ley General de Protección de Datos (Ley No. 13.709)
Chile	Ley de Protección de la Vida Privada (Ley No. 19.628)
Colombia	Ley Estatutaria de Protección de Datos (Ley No. 1.581)
Costa Rica	Ley de Protección de la Persona frente al Tratamiento de Datos (Ley No. 8.968)
México	Ley Federal de Protección de Datos Personales en Posesión de los Particulares
Perú	Ley de Protección de Datos Personales (Ley No. 29.733)
Uruguay	Ley de Protección de Datos Personales y Acción de Habeas Data (Ley No. 18.331)
Ecuador	Ley Orgánica de Protección de Datos Personales (Ley No. 19.628)
Panamá	Ley de Protección de Datos Personales (Ley No. 81)




#include <stdint.h>
int main(int argc, char **argv) {
uint64_t src = argc;
uint64_t dst;
__asm__ volatile(
"lzcnt %1, %0\n"
: "=r"(dst)
: "r"(src)
: "cc"
);
return (int)dst;
}
#define ASM_VMX_VMREAD_RDX_RAX ".byte 0x0f, 0x78, 0xd0"
static __always_inline unsigned long vmcs_readl(unsigned long field)
{
unsigned long value;
asm volatile("1: vmread %2, %1\n\t"
__ex_clear(ASM_VMX_VMREAD_RDX_RAX, "%0")
: "=rm"(value) : "d"(field) : "cc");

Geopolítica y Ciberseguridad

En la era digital, las amenazas a la seguridad de los países tienen un nuevo territorio de conflicto, el ciberespacio. A la par, se impone otra dimensión en la estrategia política. ¿Cómo avanzan los países líderes?

La amenaza de ataques a los países sigue generando una carrera contrarreloj entre las grandes potencias del mundo para desarrollar las armas más sofisticadas. Sólo que, en el siglo XXI, uno de los escenarios por excelencia es el ciberespacio y la consigna propone el desarrollo de un arsenal de defensas cibernéticas.

Hoy, la información es la reina, y protegerla es esencial. Por eso, la dimensión geopolítica es un capítulo estratégico de la ciberseguridad. Las grandes potencias dedican importantes recursos para garantizar la seguridad nacional y sus sistemas de información, intentando estar un paso más delante de las amenazas, que evolucionan al ritmo de los constantes procesos de transformación digital.

Vulnerabilidad global

Los virus y *malware*, el *phishing*, los ataques de denegación de servicio, los ataques de contraseña y el *ransomware* son algunas de las amenazas más comunes, que utilizan individuos malintencionados, espías corporativos u organizaciones criminales. Según datos de Cybersecurity Ventures, fuente confiable sobre cibereconomía global, se estima que para 2026 el costo a nivel mundial de los delitos informáticos ascenderá a US$20 billones.

En enero de 2023, el Foro Económico Mundial (WEF, por sus siglas en inglés) publicó su "Global Cybersecurity Outlook 2023", elaborado en colaboración con Accenture, que informa sobre una encuesta a 117 líderes mundiales de 32 países y 22 industrias. El resultado indica que el 91% de los encuestados opinó que un evento cibernético catastrófico y de gran alcance era al menos algo probable en los próximos dos años, mientras que el 43% dijo que un ataque cibernético ocurriría.

Con la vulnerabilidad mundial a sólo un clic de distancia, la industria tiene grandes retos para construir un terreno más seguro para individuos, empresas, organizaciones, gobiernos. El condimento global, con ataques cibernéticos que no conocen fronteras, debe sumar un tema extra: la cooperación internacional.

Muchos países están a la altura de las circunstancias a partir de la implementación de programas para minimizar riesgos y leyes para mejorar las salvaguardas de ciberseguridad. A continuación, algunos ejemplos.

Singapur, Estados Unidos y España

En la última edición del Índice de Ciberseguridad Global, publicado por la Unión Internacional de Telecomunicaciones (UIT), organismo especializado de las Naciones Unidas (ONU), se informa cuáles son los países con mejor ciberseguridad a nivel mundial.

Se destacan las acciones de Singapur, que implementó políticas sólidas, regulaciones y programas de capacitación para proteger sus infraestructuras críticas y promover la conciencia sobre la ciberseguridad.

Estados Unidos adoptó medidas para proteger su infraestructura, fortalecer la seguridad de los datos y promover la educación en ciberseguridad. La Ley de Intercambio de Información sobre Ciberseguridad (CISA) permite el intercambio de información de tráfico de Internet entre el gobierno federal y las empresas de tecnología. La regulación local de algunos Estados castiga a las empresas por fallos de seguridad cibernética. Las compañías invierten proactivamente en ciberseguridad para evitar tanto la pérdida de reputación como económica.

Y en el Top 3 también se incluye a España, que tiene una estrategia nacional y una serie de iniciativas para proteger sus infraestructuras críticas y fomentar la cooperación público-privada y la capacitación. Cuenta con una sólida regulación en materia de protección de datos.

Reino Unido, Estonia y China

Reino Unido tiene numerosas leyes sobre aspectos cibernéticos. Se destacan la Ley de Protección de Datos y el Reglamento de Privacidad y Comunicaciones Electrónicas para los proveedores de servicios de telecomunicaciones. Existen sanciones importantes para empresas negligentes. El gobierno aborda dicho riesgo mediante un Centro Nacional de Seguridad Cibernética (NCSC), que debe proteger los servicios críticos, gestionar incidentes importantes y mejorar la seguridad con tecnología y asesoramiento.

Estonia encara la ciberseguridad como parte de una seguridad integral, en el contexto de la Organización del Tratado del Atlántico Norte (OTAN) y la seguridad nacional. Cuenta con una identificación e identidad digital para cada ciudadano que permite el acceso a los servicios públicos en línea. Busca aplicar el derecho internacional a los conflictos.

La República Popular de China implementó un proyecto de ciberseguridad basado en una mayor intervención estatal. Sus estimaciones reflejan la idea de una comunidad de ciberespacio de destino común, cuyo núcleo se basa en el respeto a la soberanía cibernética de cada nación, y la necesidad de establecer directrices para el ciberespacio mediante una amplia cooperación intergubernamental.

Desarrollo e inversión

Dinamarca, Finlandia, República de Corea, Nueva Zelanda, Islandia, Suecia, Australia,

Estonia, Países Bajos y Estados Unidos encabezan el top 10 de gobierno electrónico en 2022, según datos del Índice Global de Innovación, de la ONU. Por otra parte, la Unión Europea cuenta actualmente con la Ley de Seguridad Cibernética aprobada en junio del 2019, que fortalece las medidas de ciberseguridad de los productos, servicios y procesos digitales en toda la UE.

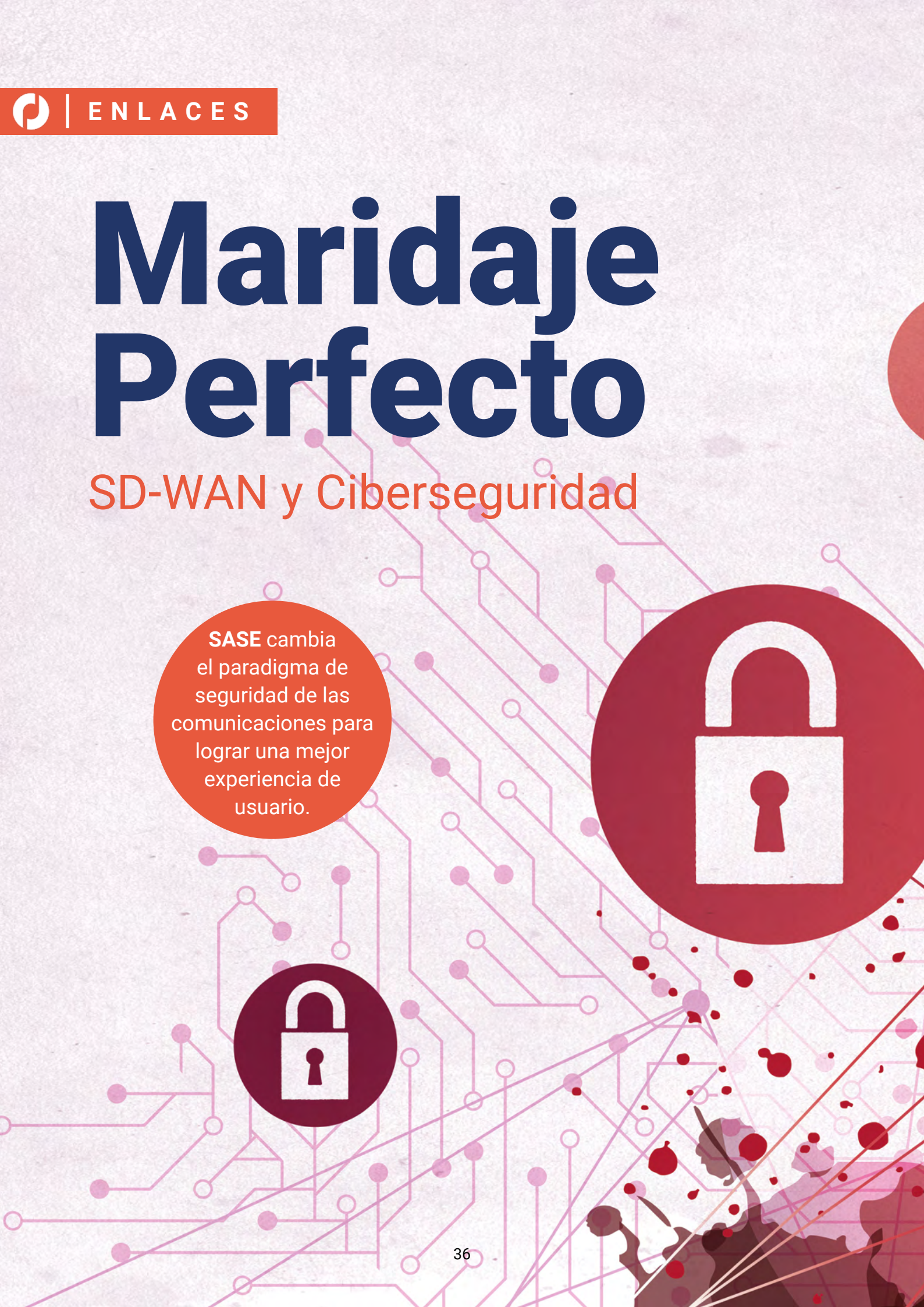
¿Qué tienen en común los países que se aggiornan en la materia? Madurez Digital. Desarrollan un compromiso con la innovación digital; impulsan la accesibilidad y la inclusión, la participación ciudadana y la prestación de servicios, por ejemplo, con la identificación digital o los servicios tributarios en línea; promueven la ciberseguridad, la privacidad de los datos y una legislación acorde; avanzan con la cooperación internacional y el intercambio. Y algo no menor: invierten en ciberseguridad para respaldar el desarrollo y la innovación de empresas y sociedades.

Los países en general, incluidos los de Latinoamérica, van adaptando leyes y normativas vinculadas a la ciberseguridad para adecuarse al vertiginoso mundo digital, sin embargo hay mucho por hacer aún.

Maridaje Perfecto

SD-WAN y Ciberseguridad

SASE cambia el paradigma de seguridad de las comunicaciones para lograr una mejor experiencia de usuario.



El vino correcto puede hacer que una exquisita comida se transforme en una experiencia inolvidable. De eso se trata el maridaje en el ámbito culinario, una práctica que está en pleno auge y tiene el objetivo de crear sensaciones nuevas, tanto en la degustación de la comida como de la bebida que acompaña. Y, si bien encontrar la pareja perfecta no es sencillo, los expertos pueden recomendar combinaciones que funcionan de maravilla para los paladares más exigentes.

En materia tecnológica, hoy, con la digitalización, el teletrabajo y las conexiones multidispositivo, los sistemas de seguridad tradicionales no son suficientes. A medida que los usuarios se conectan desde cualquier lugar y acceden a datos confidenciales en la nube, surge la necesidad de mejorar el rendimiento de las aplicaciones y aumentar la seguridad de la red. Con la transformación digital, la seguridad se traslada a la nube. Así nace la necesidad de servicios convergentes para reducir la complejidad, mejorar la velocidad y la agilidad, habilitar las redes multinube y proteger la nueva arquitectura.

Entonces se crea otro ejemplo de “maridaje” que rinde buenos frutos: Secure Access Service Edge (SASE), una arquitectura de red que dirige de manera inteligente el tráfico a la nube y realiza una inspección de seguridad avanzada, a través de la combinación de SD-WAN (Software Defined Wide Area Network, por sus siglas en inglés) con funciones de seguridad confianza cero nativas de la nube. De esta forma, S-WAN y Ciberseguridad afirman su compromiso proporcionando un viaje de acceso directo y seguro, que conecta usuarios, sistemas, puntos de conexión, redes remotas y aplicaciones.

Su foco está en optimizar la conectividad, proteger los datos y simplificar las operaciones, proporcionando seguridad completa para empresas y usuarios, que están protegidos independientemente de donde trabajen.

Experiencia SASE

Para encarar la propuesta de SASE es necesario establecer una estrategia para definir las aplicaciones que pueden migrar a la nube, asegurar los datos, transformar la infraestructura y capacitar al equipo para actuar en consecuencia.

Con su arquitectura tecnológica, las empresas pueden habilitar un acceso móvil y remoto más seguro; reducir costos y complejidad; limitar el acceso según la identidad del usuario, el dispositivo y la aplicación; y aumentar la eficacia del personal de seguridad y de la red con una gestión centralizada, entre otras funciones.

Según los expertos, el objetivo se puede resumir en la consigna de las "3 C":

- **Conectar:** cualquier usuario, dispositivo u aplicación de manera automática, simple y segura.
- **Controlar:** a partir de la concepción "confianza cero", permitir el acceso a aquellos dispositivos que apliquen a los parámetros establecidos.
- **Converger:** convivencia entre una conectividad ágil y segura.

El teletrabajo y la transformación digital modificaron los perímetros de seguridad que ofrecían los entornos de oficinas cerrados, por eso las necesidades en términos de ciberseguridad fueron evolucionando. En esta coyuntura aparece SASE.

La Guerra Fría de la Ciberseguridad

En este artículo, el autor habla de la compleja trama de los ataques cibernéticos y cómo protegerse de las amenazas en tiempo real.

por **Fabio Sánchez**
Director de Prácticas de Ciberseguridad, OCP TECH

En Ciberseguridad se ven avances más rápido que en otras industrias o sectores de Tecnologías de la Información (TI), impulsado principalmente por una economía de guerra oculta, similar a la Guerra Fría de los años ´90. Esta guerra fría en Ciberseguridad, que se viene disputando desde hace ya algunos años, no ocurre entre países, sino que está protagonizada por grupos muy bien organizados de ciber terroristas, quienes tienen objetivos muy diversos, y llevan a las empresas de tecnología y prestadores de servicios a incursionar aún más en Ciberdefensa, innovar y desarrollar servicios y soluciones enfocadas en identificar y protegerse contra un sin número de amenazas cada vez más sofisticadas. A la par, crece el uso de servicios de nube, el volumen de datos generados a diario, el acceso desde diferentes dispositivos móviles, computadoras portátiles y dispositivos inteligentes, con alta interconexión.

No es coincidencia entonces que, en términos de ciberseguridad, todas las analogías y metáforas apunten a escenarios de guerra, que nos colocan en una instancia puramente defensiva contra atacantes invisibles en un terreno digital que se ha expandido a un ritmo vertiginoso. Con esta realidad, es más difícil defender las fronteras, colocar controles en los ingresos y salidas a Internet y, para muchas organizaciones, se ha convertido en un terreno desconocido incluso dentro de sus propios ámbitos. Muchas de las acciones y soluciones en el mercado se basan en ayudar a las organizaciones a dar visibilidad y entendimiento de lo que está sucediendo en este entorno de montañas y valles digitales, muy similar a la revolución que enfrentamos a principios de la Segunda Guerra Mundial, con la implementación del radar, que cambió las reglas de juego. El radar proporcionó a las Fuerzas Militares una capacidad sin precedentes para detectar y rastrear objetos enemigos a distancias mucho mayores que antes. De la misma forma, las soluciones de ciberseguridad enfocadas en brindar visibilidad y observabilidad han dado un nuevo panorama del escenario y superficie de acción, cambiaron las reglas del juego en la guerra digital y aportaron la capacidad de reconocer los ataques en tiempo real.

La realidad que supera a la ficción

Pero el panorama no permanecería estático por mucho tiempo, la misma velocidad y diversificación de los ataques requería mayor ingenio y agilidad para responder, y la inteligencia artificial tendría mucho que contribuir. Desde sus inicios en los años ´50 y su evolución en el comienzo del siglo XXI, fue aportando modelos matemáticos de predicción que proveían la información para detección y análisis de amenazas. Sin embargo, estas capacidades estaban limitadas a Gobiernos del Primer Mundo, con capacidades de cómputo muy altas. No fue hasta una década después, cuando nuevos métodos de aprendizaje reforzado y las redes neuronales

convolucionales con la adición de capacidades de cómputo asequibles, allanaron el camino de la nueva revolución que estamos viviendo. Hoy ya es común encontrar soluciones en el mercado que afirman el uso de inteligencia artificial en pro de la Ciberdefensa. Son muchos los métodos y varias las áreas de aplicación, desde el análisis de comportamiento, basados en modelos matemáticos predictivos con *machine learning* no supervisado para la detección de anomalías y micro anomalías de atacantes sigilosos y *malware* furtivo, que se ejecuta durante meses escaneando computadoras y servidores, exfiltrando información lentamente sin ser detectados, hasta la respuesta autónoma para bloqueos de puertos y filtrado de paquetes que responden en milisegundos al inicio de un ataque, antes de que logre penetrar o perpetrar daños en la red interna de una corporación.

La nueva guerra sin duda se está librando entre máquinas. Los seres humanos no somos más que meros espectadores en el conflicto diario, muy lejos de lo que la ciencia ficción predijo años atrás, mostrándonos en libros y películas robots armados aplastando cráneos. Esta guerra se está librando ante nuestros ojos y no la vemos. Se está desarrollando a una velocidad imperceptible.

Una nueva era ha llegado con la democratización de la inteligencia artificial, cualquier persona tiene acceso a este poder, a generar código, crear páginas de internet falsas, nuevos virus y *malware* en la palma de

sus manos. La proliferación de nuevos métodos y ataques va ser exponencial en los próximos años, enfocados tanto al usuario de a pie y organizaciones pequeñas, que antes habían pasado desapercibidas o eran poco apetecibles para los ciber atacantes, como también ataques mucho más agresivos a grandes organizaciones.

La forma en que ayudemos a estas empresas, pequeñas y grandes, a enfrentar el reto y confrontar esta guerra determinará su futuro y supervivencia. En los años venideros, las crisis económicas o sanitarias no serán las que acabarán con empresas. La crisis de la ciberguerra invisible que estamos viviendo determinará quién y cuánto sobreviva, y dependerá de cómo estén preparadas para responder y recuperarse rápidamente.

Táctica y Estrategia

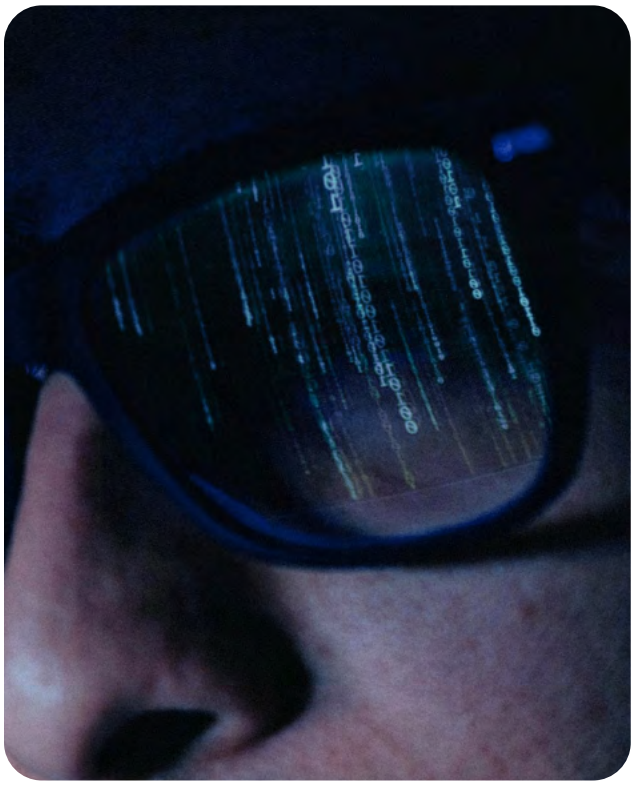
Cómo prepararse y cómo verificar el estado y madurez es uno de los desafíos que llevamos hoy en OCP TECH para acompañar a las empresas a determinar sus aspectos débiles y aconsejar en arquitecturas de acuerdo con el tamaño y razón de ser de la organización, en entornos híbridos o *full cloud*. En primeras instancias, damos foco en dimensiones tan obvias y, a la vez, tan ignoradas, como identificar, proteger, detectar, responder y recuperar.

Con respecto a la identificación, se trata de implementar un proceso y plataforma para el reconocimiento de activos de información, *software*, *hardware* que deben protegerse. Hay que categorizarlos de acuerdo a la importancia, criticidad y confidencialidad e información que manejan. Logrando esta visibilidad y gestión, se podrá avanzar y enfocar recursos en detección y protección. Caso contrario, las organizaciones están ciegas y será muy difícil recuperarse ante un ciberataque.

La etapa de detección propone plataformas de localización segmentadas para descubrir pérdida o movimiento de información en la red interna y nubes públicas, hallar movimientos y comportamientos anormales de usuarios que pudieran vulnerar sus credenciales y accesos, permitiendo a ciber atacantes permear en la organización, buscando camino hacia servicios críticos.

La protección de las personas se puede activar mediante campañas de concientización y capacitación en Ciberseguridad; y con herramientas para resguardar sus accesos mediante un gobierno de identidades centrado en las personas y su función en la organización. A la vez, se realiza con una gestión adecuada de las cuentas con altos privilegios y el acceso a plataformas críticas de la organización, y una gestión y gobierno de la información y de los datos, tanto en dispositivos de uso personal como servidores de bases de datos en nube, en *datacenters* o repositorios de terceros, y la misma transferencia de esa información desde y hacia entornos de nube, red interna e internet.

Si se miden las capacidades y se trabaja para crecer en cada una de estas áreas, será más difícil el acceso a las personas, datos, *software* y *hardware*, sin importar el tamaño de la organización, ya sea pequeña, mediana o grande, y de esta forma estaremos más cerca de ganar batalla por batalla en esta ciberguerra del nuevo siglo.



Un día en la vida de ...

Ilustración:
Santiago Guerrero

… Andrés Quinn

COO, OCP TECH

¿Quién rehúsa la fantasía de vivir un día la vida de alguien más? En conversación con este reconocido líder de OCP TECH entramos al universo de un Chief Operations Officer. Te invitamos a descubrir su visión, experiencia y forma de llevar adelante una tarea que requiere el equilibrio entre pensamiento expansivo y acción planificada.

¿Qué significa para un COO una alarma a primera hora del día?

Significa que arranco el día. Lo primero que intento es hacerme de la mayor información relevante de cada tema, para tomar la decisión más acertada en el menor tiempo posible.

Somos una compañía que al cierre de esta edición opera en 15 países, cada uno con su realidad y en más de un huso horario, así que estamos constantemente adaptándonos a lo que nos toca enfrentar.

¿Cuál sería la mejor metáfora para describir un día típico laboral?

Todos los días son distintos. Esta expansión "triple dígito anual" realmente es vibrante. Te diría que la mejor representación es un auto de competición, donde los detalles y el trabajo en equipo coordinado hacen que se llegue a la meta.

¿Cuáles son tus principales responsabilidades en esta posición?

Tengo a mi cargo el crecimiento, desarrollo, cumplimiento y superación de objetivos de todas las áreas que son parte de la operación. Soy un director de orquesta, me encanta liderar. A la vez, toda mi gestión va de la mano de un *team* sobresaliente de trabajo, con expertos en cada área y, para destacar, un equipo de Ingeniería, absolutamente envidiable.

Las áreas dentro de mi órbita son: Ingeniería de Pre y Post Venta, Delivery, con la PMO, Customer Experience, Ventas, BDM's con las BU's, *cross* a toda la organización, Comunicación y Marketing.

¿Cómo divides tu tiempo entre las diferentes funciones de trabajo?

Desde mi punto de vista, es importante tener una agenda bien ordenada y un plan con objetivos,

roles y responsabilidades bien claro. Esta organización ayuda al foco en el corto plazo y en la ejecución diaria. Por supuesto, muchas cosas no están contempladas en ella, ahí es donde se pone entretenido y la eficiencia pasa a jugar un rol fundamental para poder hacer todo lo propuesto.
En la compañía contamos con procesos calibrados y una práctica bien madura, los sistemas ayudan a ello. Las reuniones recurrentes *cross* áreas y estar abierto siempre al diálogo, a escuchar atentamente, te ayuda a anticiparte. Luego, generalmente, uno le dedica más tiempo a lo que hace naturalmente más fácil.
Es ahí cuando ese orden en la agenda te pone en eje y te hace balancear los tiempos con todas las actividades.

> *La realidad de cada uno de los distintos países, con su situación política y económica es un gran desafío externo diario.*

¿Cuáles son los desafíos más importantes que enfrentas diariamente?
La realidad de cada uno de los distintos países, con su situación política y económica es un gran desafío externo diario.
A nivel interno diría que este crecimiento en negocios, países y empleados, lo hace muy divertido y desafiante. Intentar contener a los equipos es fundamental en un ambiente de tanto crecimiento; a veces, esa vorágine, se siente. A la vez, y de la mano del departamento de Compliance, nuestras certificaciones ISO ayudan a no desordenarnos por acelerar.

De haber una muy buena noticia, ¿cuál sería?
Seguir impactando con proyectos de alto valor para la sociedad, las empresas, las personas y continuar creciendo como lo hacemos en todos los países en que operamos. Continuar alcanzando reconocimientos regionales de los socios estratégicos, como fabricantes y clientes, es una gratificante señal de esto. Me encanta ganar, realmente lo disfruto.

Describe un momento de distensión o juego durante la jornada laboral.
Me gusta mucho salir de la oficina, tomar un café en algún bar, en cualquiera de los países que tenemos presencia y volver renovado unos minutos después, con las ideas claras y habiendo sacado el foco a la inmediatez.
En Argentina en particular, disfruto mucho los asados recurrentes en la terraza de una de las oficinas de Buenos Aires, donde compartimos algunos KPI's con el equipo y se disparan conversaciones con integrantes de todas las áreas. Son encuentros informales, estamos parados, moviéndonos de un grupo a otro, tomando rápido contacto y absorbiendo información; me parece súper enriquecedor y lo veo como una tarea bien distendida. Aprendo mucho de todos los miembros del equipo, de las distintas miradas, los distintos momentos de carrera de cada uno y dónde está el foco de cada persona.
Me enorgullece el equipo que tenemos.

¿Cómo ha cambiado el papel del COO en los últimos años y con la incorporación de tecnología?
Nuestra industria es la tecnológica....así que Operaciones siempre se vinculó mucho a los sistemas, procesos y a la maximización de las herramientas tecnológicas para hacer cada vez más eficiente nuestro trabajo. Veo al COO como un líder imprescindible en la estructura, que marca el ritmo de las áreas que están en contacto con el cliente.
En otras industrias adyacentes, el rol de Operaciones está más enfocado en resolver problemas con algo menos de dinamismo, en roles más vinculados al reporte, logística y cadena de suministros.

¿Qué papel juega el COO en la innovación de la empresa? ¿Cuándo es importante no innovar?
La innovación es algo que personalmente me atrapa, pero además, por nuestro enfoque, estoy en contacto permanente con las nuevas tecnologías y en interacción constante con los líderes de nuestras BU's de soluciones y de departamentos técnicos, intentando ayudar a lograr las mejores alianzas del mercado con una mirada complementaria de negocios.
Como compañía tenemos una estrategia de profundidad en la relación con los fabricantes de la mano de una ingeniería de alto valor y muy bien capacitada, apalancada en múltiples certificaciones de nivel internacional. Estar atento y en relación frecuente con el área de Ingeniería permite entender cuál es el próximo paso o dónde debemos poner más foco.
Como indica cierto ingenio popular, hay que innovar cuando te está yendo bien, porque cuando los resultados no acompañan hay que sobrevivir. Para mí, no innovar no es una opción.

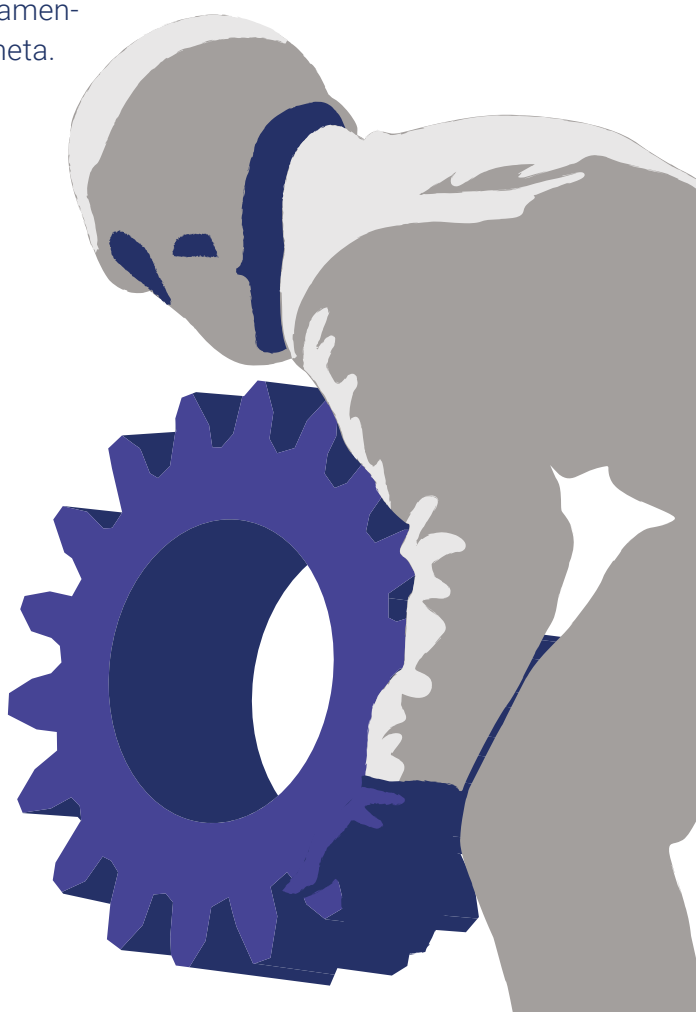
Café durante el día ¿sí o no?
Sí, siempre. Soy muy cafetero y disfruto ese corte para tomar envión.

¿Cuál fue el momento más desafiante de tu carrera como COO?
Algo que nos encanta en OCP TECH es sostener que somos una organización con mentalidad de corporación y corazón de *startup*. Esa ambigüedad de integrar las culturas sin caer en recetas repetitivas y lograr la expansión de 4 a 16 países, superando los KPI's propuestos por el CEO, ha sido un desafío realmente espectacular que guardaré por siempre en mi haber profesional.

En tu visión, ¿qué es lo más importante que debe tener un COO para tener éxito?
Apasionarse con lo que hace, conformar un equipo alineado de quien aprender y donde impactar todos los días. Contagiar entusiasmo, ser generoso con la experiencia y tener la habilidad de valorar los logros ajenos; es siempre "entre todos".

¿Usas IA generativa en tu gestión diaria? ¿Para qué?
Algunas de las soluciones que ofrecemos tienen IA como parte de su innovación. Hay que estar muy atento a estos aprendizajes, ya que en varios aspectos hace un gran diferencial: lo veo muy marcado en la atención a clientes, en la inmediata implementación de soluciones tecnológicas y la inmensurable eficiencia que se logra.

Algo más que quieras agregar y que no te haya preguntado.
Me gustaría destacar un par de cosas que para mí tienen un rol clave en el éxito de OCP TECH. Por un lado, la visión de Leo (Leonardo Scatturice), nuestro CEO, quien vio claramente hace unos años la posibilidad de desarrollar un integrador de alto valor agregado para profundizar en las tecnologías más importantes del mercado y el impacto de las soluciones en la gente. Un empresario tenaz y visionario, un gran líder que nos da libertad absoluta de acción, confiando en nuestras decisiones y permitiéndonos hacer. Por otro lado, un tremendo equipo de trabajo con ganas de superarnos en todos los ámbitos. Ambos, líder y equipo, somos un motor inagotable de energía que valoramos cada paso, cada logro y vamos siempre por más hasta alcanzar exitosamente la meta.



Sustentabilidad centrada en las personas

por **Verónica Funes**
HR Manager, OCP TECH

Hacer uso correcto de los recursos actuales sin comprometer los de las generaciones futuras está mucho más cerca de la vida diaria de lo que podría sugerir un concepto. Particularmente, necesita de las personas y su acción responsable.

Si miramos al interior de las organizaciones, podríamos concluir que la cultura organizacional acorde con las propuestas y desarrollos externos en pos de la sustentabilidad, aporta coherencia y significado. Una estrategia es poco sostenible si detrás de ella no existe el soporte de los valores, los hábitos, los comportamientos de quienes la llevan adelante. Por eso, centrar nuestra cultura organizacional en las personas, al estilo Customer Centric, implica formar a los colaboradores en cada uno de sus roles con las habilidades que respaldarán la estrategia.

En este sentido, un modelo que me resultó muy útil tanto en OCP TECH como en otras compañías es el de las 3 H: Humildad, Humanidad, Humor.
Veamos en detalle qué comportamientos promueve cada una.

3 H para sostener lo sustentable

Humildad

- Ser tolerante con los distintos puntos de vista.
- Aceptar la diversidad.
- Mantener una comunicación abierta coherente entre el afuera y el adentro de la organización.
- Alentar el aprendizaje continuo.
- Ser reflexivo con uno mismo.
- Reconocer nuestros errores y aprender de ellos.
- Dar las gracias y pedir disculpas.

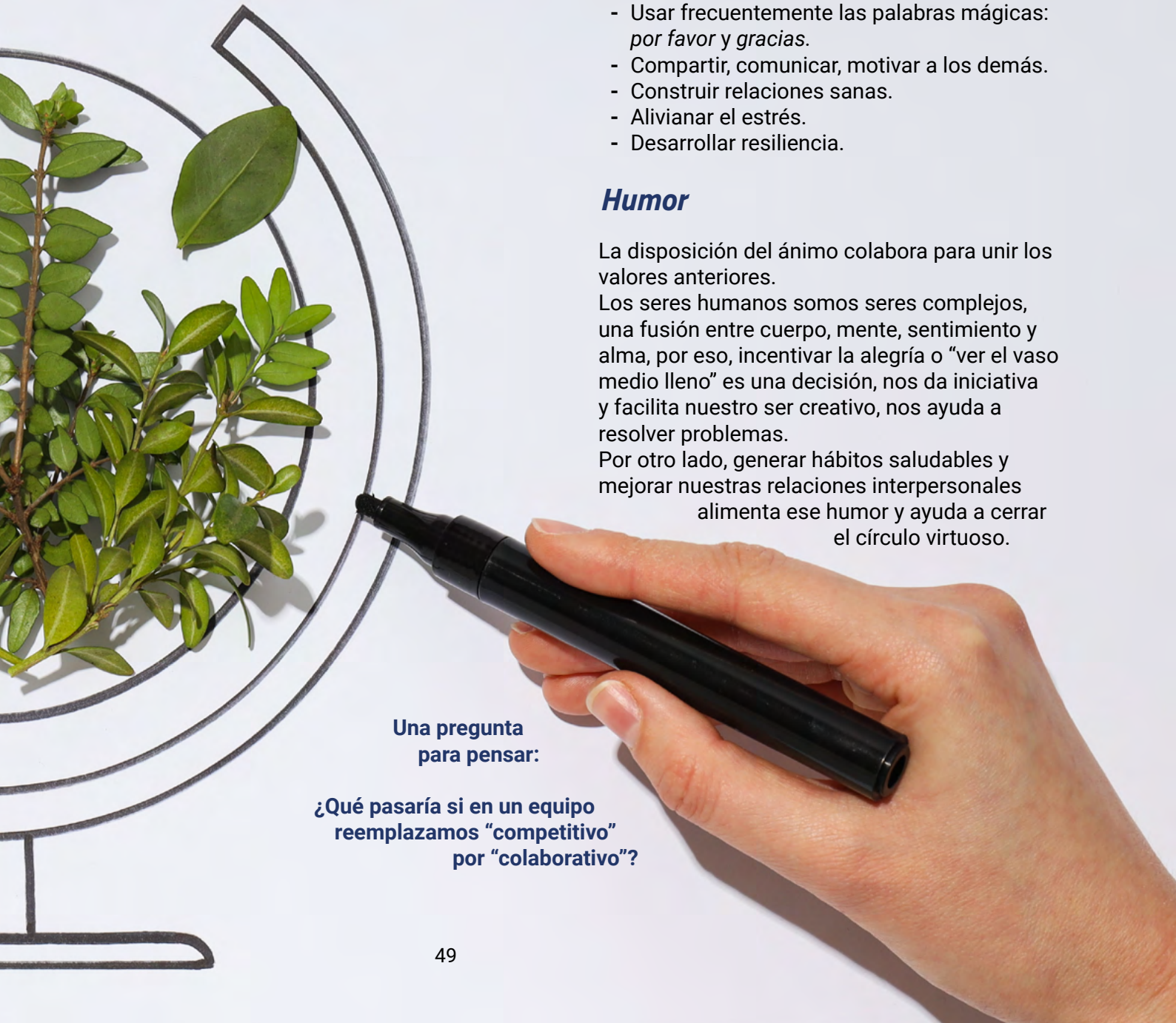
Humanidad

El desarrollo de la tecnología está generando un aluvión que nos arrastra, y la diferencia que podemos aportar es nuestro lado más humano: la generosidad, por ejemplo. Otras capacidades a desarrollar son:

- Empatía.
- Confianza.
- Ética en el trabajo.
- Respetar a los demás.
- Ser cercanos y sensibles con quienes nos rodean.
- Usar frecuentemente las palabras mágicas: *por favor* y *gracias*.
- Compartir, comunicar, motivar a los demás.
- Construir relaciones sanas.
- Alivianar el estrés.
- Desarrollar resiliencia.

Humor

La disposición del ánimo colabora para unir los valores anteriores.
Los seres humanos somos seres complejos, una fusión entre cuerpo, mente, sentimiento y alma, por eso, incentivar la alegría o "ver el vaso medio lleno" es una decisión, nos da iniciativa y facilita nuestro ser creativo, nos ayuda a resolver problemas.
Por otro lado, generar hábitos saludables y mejorar nuestras relaciones interpersonales alimenta ese humor y ayuda a cerrar el círculo virtuoso.



Una pregunta para pensar:

¿Qué pasaría si en un equipo reemplazamos "competitivo" por "colaborativo"?

¿Cómo mantener la **“humanidad”** en la era tecnológica?

En un mundo donde la tecnología sorprende con sus avances y las empresas buscan constantemente la innovación, la Responsabilidad Social Empresaria se alza como un pilar fundamental para reorganizar estrategias que prioricen la construcción de una sociedad más sostenible y equitativa.

La cultura corporativa y los valores humanos pueden marcar la diferencia en un mundo impactado por la tecnología. OCP TECH -una compañía que busca aportar valor en su propia organización, en el negocio de sus clientes y proveedores, y en la comunidad en general- entiende que la Responsabilidad Social Empresaria (RSE) es clave para que personas y empresas prosperen en un mundo cada vez más digitalizado. La tecnología brinda un alcance de gran impacto, su magnitud no tiene precedentes, su vigencia se sostendrá en el futuro, por eso, la ética y las habilidades sociales asociadas a esta disciplina adquieren aún más relevancia.

OCP TECH es la primera empresa latinoamericana en recibir la Certificación Anticorrupción y posee Certificación de Empresa Inclusiva.

Visión compartida

¿Qué es la RSE? Hoy, en general, las empresas, además de generar utilidades, reconocen que sus actividades impactan la calidad de vida de sus empleados y de su comunidad, por eso, se ocupan de que sus operaciones sean sustentables en lo económico, en lo ambiental y en lo social. Más allá de su tamaño, el sector al que pertenece o su nacionalidad, tienen una visión compartida que integra la ética, la transparencia y el respecto por las personas, ya sean accionistas, empleados, proveedores, clientes o la sociedad en su conjunto.

Las organizaciones relacionadas con la tecnología, una herramienta que revolucionó nuestras vidas y las formas de hacer negocios, tienen claro las ventajas que trajo aparejada, entre otras, rápido acceso a la información, se facilita el aprendizaje, aumenta la productividad, se rompen las barreras de las distancias; y también los obstáculos a superar y su rol en esta tarea. Más allá de las cualidades de los productos o servicios tecnológicos, su utilización ejerce una huella sobre las personas o los colectivos de ciudadanos. El uso constante de teléfonos inteligentes, computadores portátiles y otras tecnologías incide perjudicialmente sobre un cuerpo humano sedentario.

Entonces, **¿cómo impulsar la salud física y mental?** Hoy, las nuevas tendencias proponen llevar la RSE hacia caminos más integrales.

Manos a la obra

Desde OCP TECH buscan explorar enfoques innovadores que utilizan la tecnología para promover un estilo de vida más activo y saludable. Si se quiere mantener la longevidad, se requiere tener un cuerpo en movimiento. Este proceso ya comenzó tanto desde el Gaming como desde el Metaverso. En un futuro, se podrían incorporar sentidos, como el gusto o el olfato.

Los proyectos de OCP TECH se desarrollan en los sectores público, privado y académico y abordan también a las instituciones intermedias. Trabaja en distintos proyectos con el Ministerio de Educación, el Gobierno de la Ciudad de Buenos Aires, la Universidad de Buenos Aires (UBA), la Universidad Tecnológica Nacional (UTN), la Universidad Nacional de San Martín (UNSAM), Instituto Tecnológico de Buenos Aires (ITBA), Universidad de Belgrano (UB), Universidad Católica Argentina (UCA), y en distintas instituciones deportivas para acercar la tecnología al deporte, entre otras.

La tecnología puede ser un aliado en el recorrido del ser humano, si se utiliza con sabiduría para promover valores y el bienestar general.

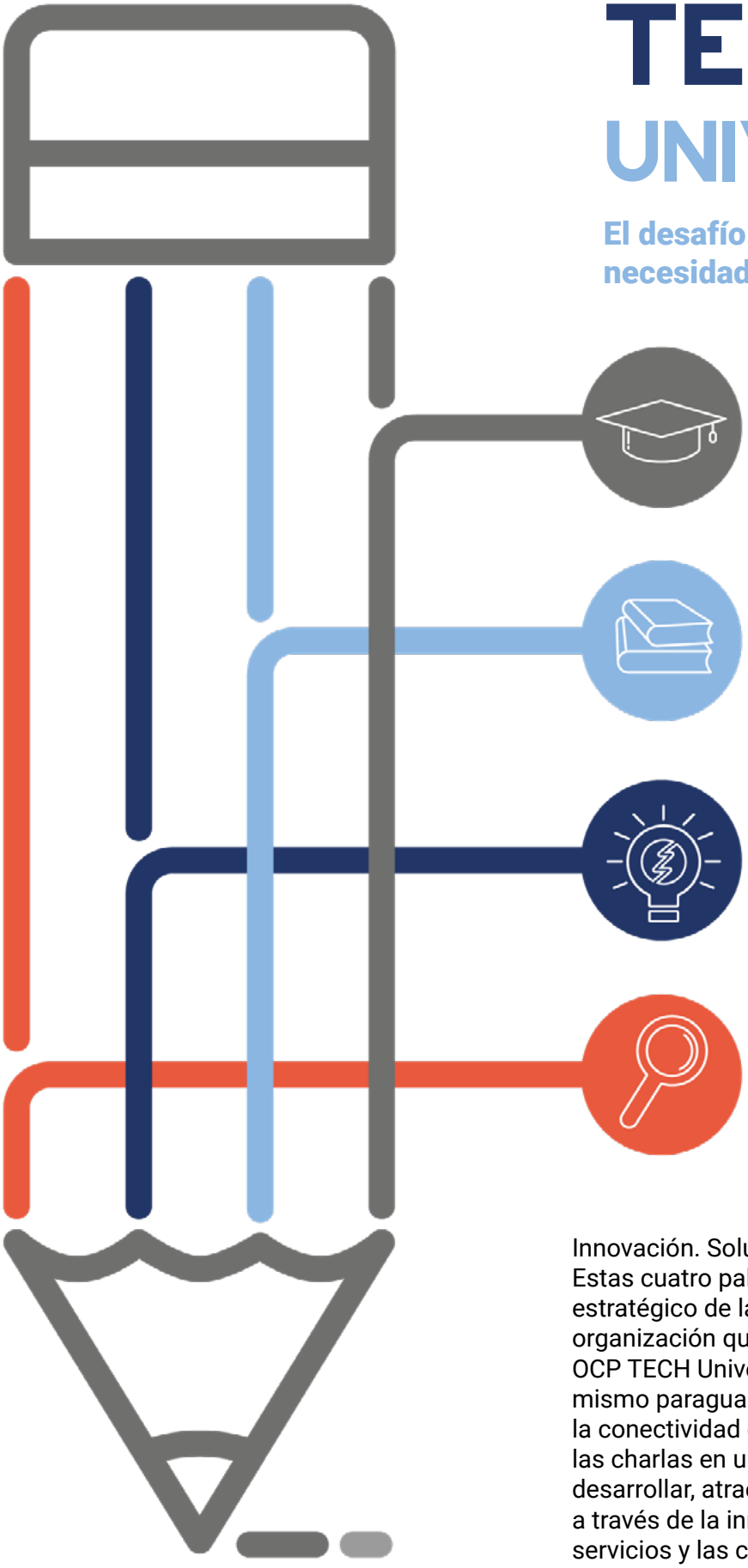
Huellas

por **Karina Basanta**

Desafío
Entrar en la instancia donde lo cómodo
se desparrama en lo intrépido de la experiencia
Brindarnos en colaboración
Salir hacia el otro, encontrarlo
Proponer la mejor versión de lo nuestro
Hacer con impacto
Impacto positivo
Impacto certero
Impacto deslizante y extendido
Si hubiera una metáfora del entendimiento
¿Cuál sería?
¿Y del sé como hacer para colaborar con tu éxito?
Si hubiera una metáfora de la satisfacción
habría que desplegarla ahora.
Porque la fantasía entre nuestras organizaciones
debe ser compatible
Para realizarse
Con la simpleza de lo unificado

OCP TECH UNIVERSITY

El desafío es adaptarse a las necesidades del mercado laboral



El futuro del trabajo presenta retos, y también oportunidades. Para aquellos que están dispuestos a aprender y reinventarse, OCP TECH impulsa el aprendizaje continuo, la capacitación y el desarrollo de habilidades.

Innovación. Soluciones. Integración. Ingeniería. Estas cuatro palabras representan el foco estratégico de la empresa OCP TECH, una organización que supo dar vida al "concepto" OCP TECH University para unificar bajo un mismo paraguas las capacitaciones internas, la conectividad con el mundo académico y las charlas en universidades. La estrategia es desarrollar, atraer y retener talento para que, a través de la innovación, la integración de servicios y las certificaciones en la ejecución, se

avance con el desarrollo, se equilibren ventajas, oportunidades y eficiencia, y se implementen las mejores soluciones en un mundo que está en constante evolución. En este sentido, OCP TECH University colabora en la creación de un círculo virtuoso de entrega y recepción de conocimiento que facilite el aprendizaje y la formación de la experiencia.

La misión y sus aplicaciones

A través de una metodología transversal y con un sistema dinámico, se busca ordenar la información interna y la externa, unificar los mundos académico y corporativo y, a la vez, ofrecer herramientas y comunicación efectiva acordes al concepto.

La estructura prioriza dos ejes temáticos:

- La capacitación a los colaboradores, a partir de diferentes programas.

- Las charlas temáticas en instituciones educativas, a fin de llevar la propuesta y acercar una visión sobre la tecnología.

La filosofía de OCP TECH University es promover una cultura de aprendizaje continuo en todos los perfiles que integran la compañía. Abarca tanto a las personas jóvenes como las más experimentadas, y les otorga ayuda para mantenerse abiertas al conocimiento y la actualización constante, adaptándose a nuevas tecnologías, metodologías, habilidades, a lo largo de sus carreras.

La agenda de capacitaciones de OCP TECH University abarca temáticas tales como:

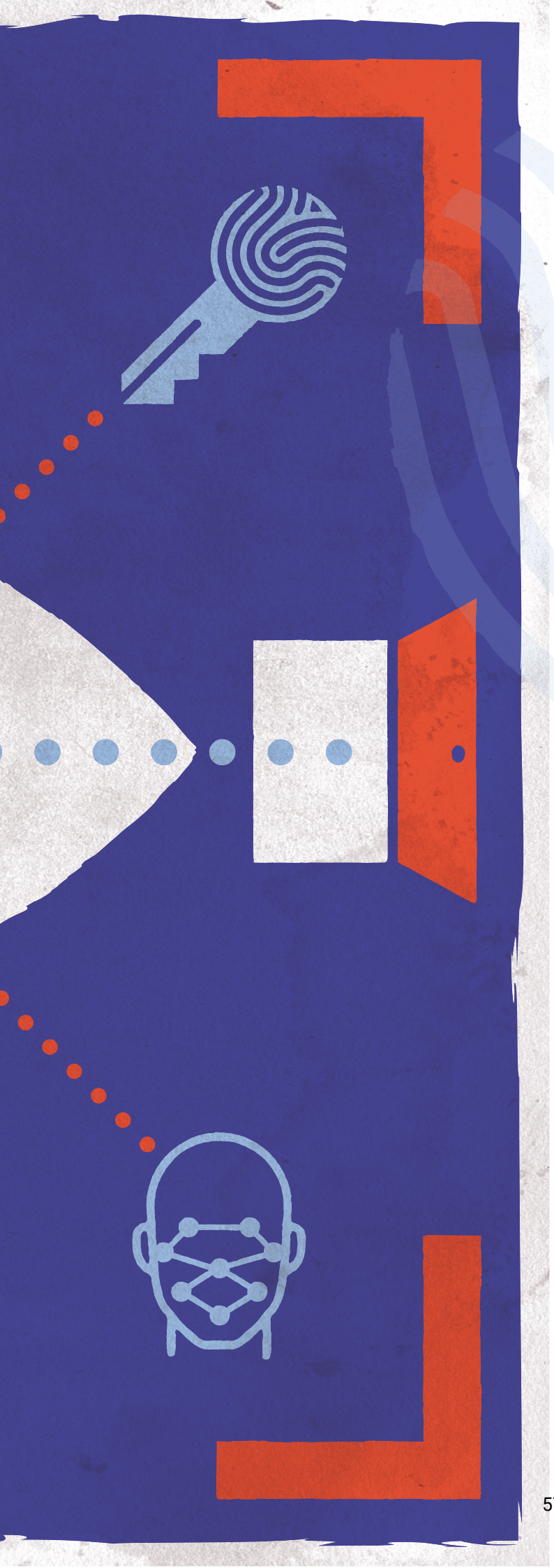
- Charlas de inducción.
- Programa de *compliance*, integrado por disertaciones de concientización sobre la política anti-soborno y certificaciones de calidad.
- Propuesta *sales school*, a cargo de un equipo interdisciplinario capaz de brindar soluciones integrales, innovadoras y con impacto social.
- Disertaciones sobre ciberseguridad, desarrollo de software, soluciones de infraestructura para nube híbrida, y de innovación, que impulsan procesos más eficientes, rentables y escalables.
- Herramientas para evaluación de desempeño.
- Programa de habilidades blandas.
- Capacitación dirigida a gerentes, para promover la selección eficaz de personal.
- Charlas sobre cómo calcular comisiones, con consejos puntuales para el nivel gerencial, entre otras.

El factor humano

Más allá de la teoría, los entrenamientos y programas están centrados en el desarrollo de habilidades prácticas que sean aplicables en el entorno laboral, tales como liderazgo, creatividad y otras competencias que hoy se requieren en la gestión diaria.

Verónica Funes, HR Regional Manager de OCP TECH, dice: “El trabajo está cambiando. Para el futuro, se necesita más potencial humano y pensamiento crítico. El valor se agrega desde lo humano”. Y subraya la responsabilidad social de generar programas de *reskilling* y de *upskilling* para ayudar a las personas a mantenerse actualizadas y adaptarse a los cambios en el mercado del trabajo.

En este proceso, la colaboración con instituciones educativas es fundamental para conectar el mundo académico con las necesidades del mercado laboral. La participación en eventos universitarios, charlas y colaboraciones educativas puede ayudar a minimizar la brecha entre la educación formal y las habilidades requeridas en la industria.



Validación biométrica de acceso seguro

Nuestras medidas biológicas y comportamientos nos identifican.

Son **propias y** únicas

A los sistemas de autenticación ya conocidos como el uso de la huella digital, el iris del ojo, la voz y el reconocimiento facial, se están sumando nuevos, tales como la forma de caminar o pararse, las venas de las manos y los aromas corporales. Avances tecnológicos al servicio de la autenticidad para el acceso seguro.

Ilustración:
Santiago Guerrero

La **identidad digital** consiste en establecer esa confianza en ambos extremos de la interacción.

La **confianza** debe estar en el corazón del sistema.

Identidad digital

por **Gabriel De Simone**
Team Principal MIAid, OCP TECH

Estamos ayudando a dar forma a un mundo donde las personas y sus dispositivos puedan interactuar digitalmente entre sí y con las organizaciones, con confianza y sin fricciones innecesarias; un mundo donde se pueda reconocer fácilmente a las personas para que puedan acceder a los servicios o experiencias que desean; un mundo en donde nuestras interacciones digitales se han vuelto multifacéticas, desde PC y teléfonos inteligentes hasta hogares, automóviles y dispositivos portátiles conectados mediante voz, tacto y presencia.

Hemos entrado en la era de la hiperconectividad, donde los servicios digitales se mezclan de manera invisible con la vida diaria de las personas. Esto nos trajo grandes beneficios como consumidores, productores, ciudadanos y seres humanos. Los servicios digitales han cambiado la forma en que compramos, hacemos negocios, accedemos a servicios de educación y salud. Por eso es fundamental establecer y salvaguardar la confianza en las interacciones digitales, de forma simple, rápida y segura.

Con los procesos actuales de autenticación, un usuario promedio puede enfrentarse a 100 cuentas de inicio de sesión que administrar, todas con enfoques dispares en cuanto a contraseñas y validación. Sin embargo, el fraude de identidad está aumentando y se ha convertido en un problema mucho mayor en línea que fuera de ella.

El objetivo de MIA es Facilitar y Restaurar la confianza en el mundo digital haciendo más simple la vida de las personas a la vez que protege a las instituciones.

Los principios de la Identidad Digital

Actualmente, las personas pagan por sus interacciones digitales con datos y privacidad. Cada día, se les pide que proporcionen información personal para poder acceder a los servicios digitales básicos.

A menudo no saben dónde se almacenan esos datos, qué tan seguros son, cómo podrían comercializarse y quién se beneficia con ellos.

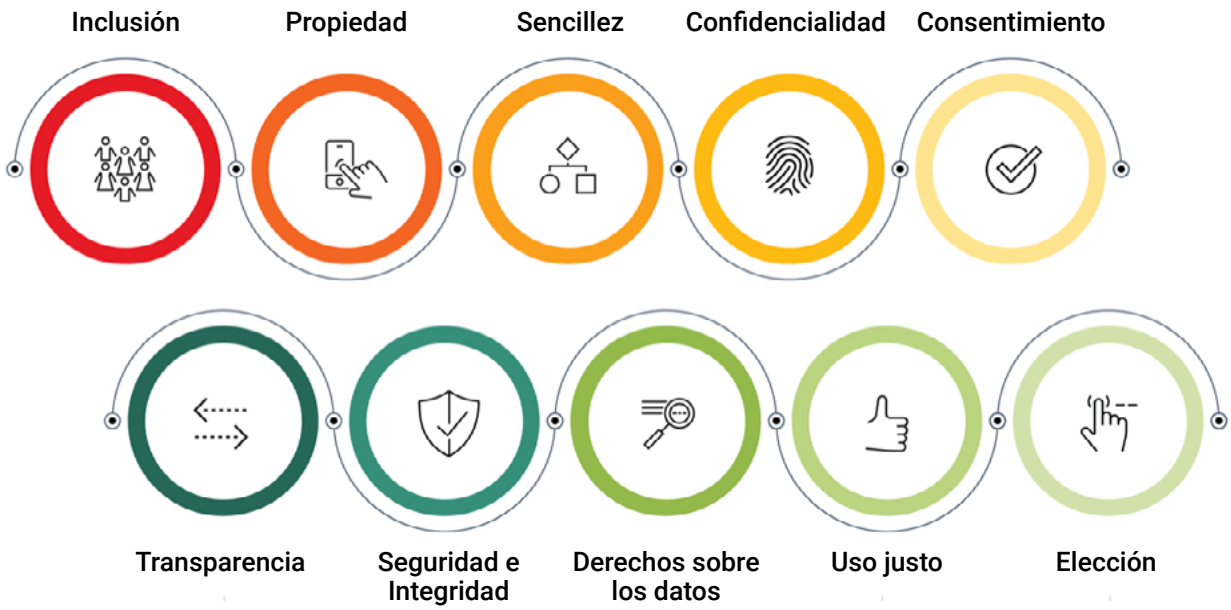
Este es un mal negocio para las personas, pero sobre todo para las empresas, bancos y gobiernos, pues a medida que los individuos se ven obligados a distribuir su información sin control no hacen más que exponer aquello que luego es utilizado para atacar cuentas privadas e información confidencial.

El mecanismo actual perjudica a todas las partes, pues hace más difícil confiar en alguien que realiza una compra, accede a un servicio o firma un documento. Entonces, todo el sistema se vuelve más complejo e inseguro. Las personas deben ir a las oficinas públicas para solicitar documentación, acceder a un beneficio o incluso hasta pedir un simple turno. Incluso comprar en línea se ha vuelto cada vez más complicado cuando se trata de bienes de alto valor, pues el riesgo implica agregar fricción a cada interacción cotidiana.

Las regulaciones de privacidad, como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, han ayudado a restaurar cierta confianza y proporcionar un entorno acogedor para las infraestructuras de identidad modernas, pero eso es sólo el principio, pues en última instancia seguimos sin estar seguros de “quién está del otro lado”.

El modelo de MIA brinda al usuario el control y aborda cuestiones de privacidad, propiedad, transparencia, seguridad, entre otras. Todo se reduce a esto: el individuo es dueño de su identidad y controla sus datos de identidad.

Colocar al individuo en el centro del ecosistema de identidad digital es esencial. Nuestros principios rectores promueven la confianza y la comprensión al tiempo que restauran el control de los datos personales al individuo.



MIA Citizen ID

Las soluciones de SSI (Self Sovereign Identity) de MIA dan al residente el control de sus propios datos y hacen que la información de identificación sea verificable de forma independiente, eliminando la necesidad de que una agencia gubernamental almacene datos confidenciales. Con SSI, el individuo decide cuánta información comparte y con quién, tal como lo hace con su billetera física y sus credenciales. Las organizaciones que solicitan identificación no retienen ninguna información personal y el usuario tiene control total sobre todo.

Por estas razones, varias agencias estatales están recurriendo a SSI para verificar de manera eficiente y segura las credenciales de las personas mientras realizan transacciones en línea, como renovar licencias de conducir, registrar vehículos y obtener licencias comerciales.

Control sobre la información personal

Con la Identidad Digital Rehusable, una persona puede compartir selectivamente sus credenciales según lo que se requiere para esa transacción. También pueden dictar cómo se utilizan esos datos y revocar el permiso para compartir datos en cualquier momento. El gobierno sólo obtiene la información que necesita cuando la necesita. Mientras que el residente mantiene control sobre su información de identificación personal (PII).

Interoperabilidad para una mejor eficiencia

La Identidad Digital Única permite mayor velocidad y seguridad. El tiempo de procesamiento se reduce sustancialmente y las agencias pueden procesar las solicitudes rápidamente. Además, los residentes se benefician de la comodidad y el servicio que esperan en su vida digital.

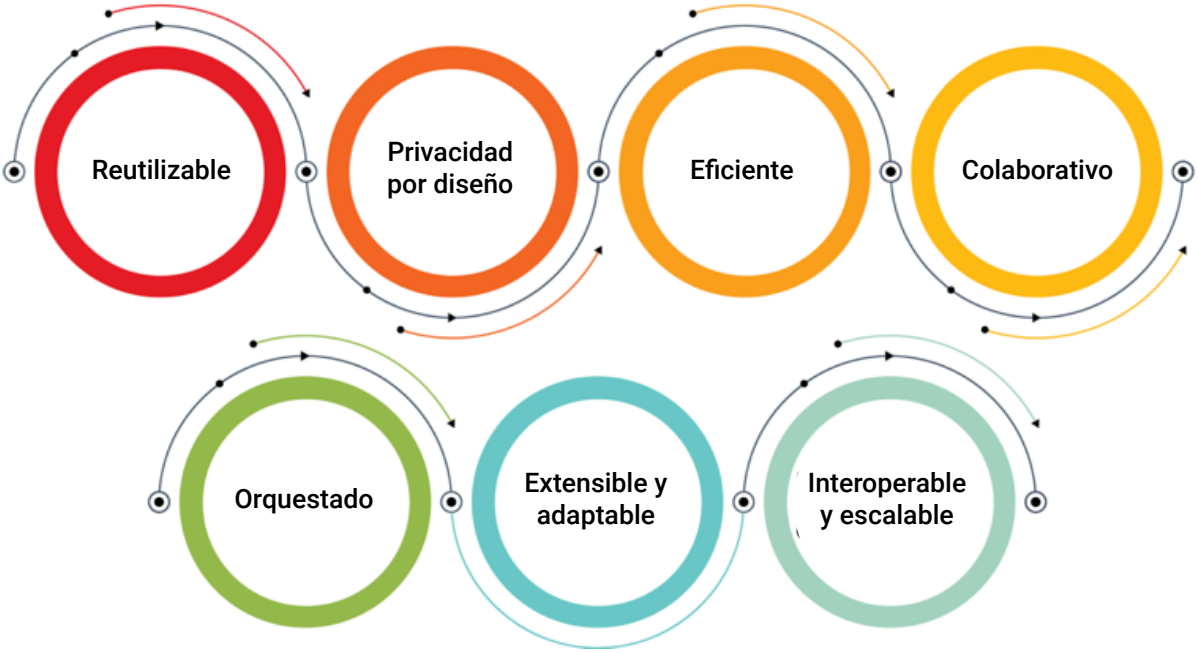
Mayor seguridad y confianza manteniendo el control de la información

MIAid permite a los gobiernos emitir credenciales en un formato estandarizado como el de SSI a través de Credenciales Verificables que, a la vez, serán firmadas por los DIDs (Identificadores Digitales Distribuidos) y autenticadas mediante el proceso biométrico de MIA. De esta forma, no se altera el proceso de gobernanza de la información, es decir, los datos siguen en el mismo repositorio gubernamental. Sin embargo ahora, el ciudadano recibe una Credencial Verificable que almacena en MIA o en cualquier Billetera que cumpla con el estándar de SSI para ser presentada en cualquier servicio privado, en cualquier parte del mundo.

Ahora su información está segura, el ciudadano tiene el control sobre ella, y sus datos están protegidos para cualquier interacción que necesite realizar con terceros.

El cambio en el modelo de Interacciones

Otros Sistemas	MIAid
Sistemas personalizados, especializados y cerrados	Servicios transparentes y globalmente interoperables
Intercambio excesivo de datos sin transparencia	Intercambio de datos controlado por el usuario
Uso de datos de identidad estáticos	Datos de identidad dinámicos y biométricos
Cientos de contraseñas vulnerables	Una identidad digital reutilizable que funciona en todas partes
Un sistema **excluyente**	Un sistema **inclusivo**



Pilares del modelo de MIA

Identidad digital interoperable y reutilizable: Elimina la necesidad de múltiples contraseñas y procedimientos de verificación de identidad. Una identidad digital permite a las personas utilizar un único medio para autenticarse en múltiples servicios digitales, que abarcan sitios web, aplicaciones, dispositivos, entre otros.

Privacidad por diseño: Permite a los usuarios proteger sus datos y experimentar transparencia en la gestión de sus vidas digitales.

Eficiente: Ser más seguro no debe ser más complejo para las personas. La eficiencia ayuda a implementar nuevos servicios de valor agregado, mejorar la participación, reducir la fricción, reducir los costos de identidad, mejorar la seguridad y cumplir con los requisitos regulatorios.

Colaborativo: Las partes interesadas, operativas y tecnológicas, cooperan para definir estándares y regulaciones.

Orquestado: Reemplaza la agregación de datos por un ecosistema orquestado de datos distribuidos.

Extensible y adaptable: Se estructura alrededor de un núcleo que se puede implementar total o parcialmente, de acuerdo con los estándares, regulaciones y normas del país.

Interoperable y escalable: Se permite una interacción segura entre las infraestructuras de datos oficiales y los participantes del sector privado, al tiempo que cumplen con los estándares definidos de funcionalidad, rendimiento, seguridad y otras regulaciones que puedan existir en los mercados locales.

Un Sistema Colaborativo permite desarrollar confianza en una transacción de identidad.

MIA actúa como un proveedor de servicios de identidad digital acreditado para brindar a todos los participantes la confianza y la asistencia que necesitan para navegar en un entorno digital complejo de múltiples partes interesadas.


OCP
TECH
INGENIERÍA DE IMPACTO

POLICÍA NACIONAL DE COLOMBIA

Resumen ejecutivo

Sector: Público.
País: Colombia.

La Organización: Conformada por 165.794 personas, el cuerpo de la Policía Nacional de Colombia comprende mujeres, hombres, uniformados y no uniformados de todas las categorías. Su misión como fuerza radica en el mantenimiento de la convivencia como condición necesaria para el ejercicio de los derechos y las libertades públicas y para asegurar que los habitantes de Colombia convivan en paz, fundamentada en el código de ética policial. Su objetivo al 2030 es ser una organización preparada para responder ante el cambio social a nivel local y global, como resultado de transformaciones estructurales que generen cultura y conciencia de futuro responsable en la ciudadanía.
La Policía acoge como Meta Grande y Audaz, la siguiente:
"Durante los primeros cuatro años cumpliremos con el servicio de policía a través de la unidad institucional para responder a los diversos comportamientos generacionales y regionales que impacten en la convivencia, mediante la innovación, el uso de herramientas tecnológicas y la optimización de recursos".

Las Unidades que conforman la Policía Nacional son:

- Policías metropolitanas y departamentos de policía.
- Direcciones y oficinas asesoras.
- Escuelas de policía.
- Unidades y grupos especializados.
- Unidad policial para la edificación de la paz.
- Oficina de control interno.
- Oficina de relaciones y cooperación internacional policial - ORECI.
- Aviación policial.
- Centro Internacional Estudios Estratégicos contra el Narcotráfico.
- Departamentos y Municipios seguros.
- Inspección General y Responsabilidad Profesional.
- Observatorio del delito.
- Ameripol de Colombia.
- Centro de estándares de la Policía Nacional.

El desafío: Lograr el acceso de todos los policías de la fuerza a las aplicaciones corporativas, desde sus dispositivos móviles y evitando el uso de *passwords* y doble factor de autenticación.

La solución: ORACLE One Time Password y MIA (Mobile Identity Access) by OCP TECH. Se trata de una combinación entre tecnología tradicional y de nueva generación.

Estado de la implementación: Finalizada.

Próximos pasos: Consolidación de servicios a través del uso de la plataforma en 2024.

MOOREA
a la vanguardia de la transformación digital

Para adentrarnos en este otro espacio de gran impacto para la compañía, conversamos con Hernán Piñero, VP Sales NOLA, OCP TECH.

¿Por qué este segmento es de interés para OCP TECH?

Nuestra plataforma Moorea representa una solución única en su segmento, especialmente para el Sector Público, en cada uno de los países en que operamos. Tiene un gran diferencial por sobre las demás plataformas de mercado: estar basada en código *Open Source*, lo cual asegura al cliente la continuidad de funcionamiento, independientemente del pago de licencia. El cliente es dueño de la solución, y de su código fuente, con lo cual puede, a futuro, generar sus propios formularios, expedientes y trámites.

¿Qué desarrollos se están llevando adelante?

Se están gestionando proyectos en varios organismos a nivel nacional y provincial en Argentina. Además, durante 2023 comenzó el proceso de posicionamiento de la plataforma en el resto de la región. Ya tenemos proyectos en marcha, POC (Proof of Concept) y demos en Colombia, Ecuador, Perú, Panamá, Guatemala y República Dominicana.

¿Cuál es el desafío a vencer?

En Argentina contamos con un nombre y un lugar reconocido para Moorea. Nuestro objetivo para el resto de la Región es tener al menos un caso de referencia en cada país para el primer semestre de 2024.

¿Cómo lo hace OCP TECH? ¿Por qué una organización la elegiría para avanzar con un proyecto de este tipo?

A diferencia de nuestra competencia, la propuesta de OCP TECH no sólo involucra la plataforma y los servicios para realizar la transformación digital o “despapelización” de los organismos, sino que también se apoya fuertemente en el plan de adopción y capacitación a clientes, liderado por el *team* de CX. Se trata de un programa a largo plazo, donde al final del camino, el cliente utiliza y aprende sobre su tecnología, llega a programar la parte visual (procesos), despliega sus propios formularios, y en caso de ser posible, inclusive, programa ciertos desarrollos simples, ya sea con personal propio, contratando colaboradores o mediante acuerdos realizados con universidades.
De esta forma, desde OCP TECH no sólo brindamos una solución tecnológica, sino que ayudamos a los Gobiernos a ser más ágiles, eficientes, transparentes y generamos puestos de trabajo de calidad.

Punto por punto

Uno de los espacios que cobró gran relevancia en las compañías durante el 2023 y que enfrenta importantes desafíos en el 2024, es el área de Administración y Finanzas. En este artículo, hacemos un punteo de los principales ejes de estrategia y gestión de estos departamentos en OCP TECH, de la mano de Fernando Antolín Dulac, Chief Financial Officer de la compañía.

En empresas tecnológicas, la expansión sostenida del mercado trae aparejadas cuestiones relacionadas a, por ejemplo, el abastecimiento de insumos o productos que den respuesta a la demanda. Si están basadas en Argentina, se suma el contexto socio económico restrictivo para girar divisas al exterior y desarrollar planes para mitigar los efectos de la inflación y devaluación de la moneda local.

Principales desafíos durante el año 2023

- Fortalecer el área de Supply Chain para permitir el abastecimiento desde proveedores locales y del exterior, como así también la logística de dichas compras hasta el cliente.
- Coordinar tareas de ComEx con áreas internas y externas para permitir pagos a los proveedores del exterior desde Argentina.
- Mejorar los cierres contables mensuales para generar informes de gestión de mayor calidad.
- Mejorar la atención a proveedores desde el sector de cuentas por pagar.
- Desarrollar actividades de inversión en moneda local para mitigar el impacto de la devaluación del peso en Argentina.
- Duplicar la frecuencia de adecuaciones de salarios para compensar efectos de la inflación en Argentina.

¿Cómo se hizo frente?

- Desarrollando procesos eficientes por sector.
- Fomentando el uso de herramientas informáticas como el ERP.
- Mejorando el liderazgo a través del desarrollo de las habilidades de los *managers* de cada sector.

- Haciendo *partnerships* con terceros expertos (fondos de inversión, por ejemplo).

¿Hubo crecimiento en el área? ¿Cómo fue?

- Ingresaron profesionales expertos en tareas funcionales (impuestos, contabilidad, abastecimiento y gestión).
- Hubo recambio de personal, sin incrementar la cantidad total de la nómina del área.
- Se realizaron procedimientos de informatización, certificación, monitoreo y control de todos los procesos.

Objetivos para 2024

- Implementar un ERP (Planificación de Recursos Empresariales, por su sigla en inglés) en la nube, para registrar las transacciones de todos los países y realizar un EEFF (Estado Financiero) consolidado en USD.
- Desarrollar objetivos por sector y generar evaluaciones de desempeño.
- Mejorar la calidad de información contable de toda la compañía.
- Capacitar a las personas del área para alentar su desarrollo profesional.

> En OCP TECH hacemos foco en el desarrollo de los colaboradores para que exploten al máximo su potencial

Fernando Antolín Dulac.

OCP TECH

1era. Compañía de Argentina certificada Anti-Soborno

En mayo de 2023, OCP TECH se convirtió en la primera compañía de Argentina en certificar la Norma ISO 37.001:2017 en Sistema de Gestión Anti-Soborno (SGAS) por parte de TÜV NORD CERT. Esta certificación coloca a la empresa como parte de un selecto grupo de organizaciones pioneras en América Latina que buscan promover un entorno responsable y transparente mediante la implementación de este estándar internacional. Bajo esta iniciativa, se priorizan el compromiso, la responsabilidad corporativa y el cumplimiento de los más altos estándares internacionales en materia de ética empresarial.

El soborno es una de las formas de corrupción más habituales en el mundo de los negocios. Las empresas y otro tipo de organizaciones pueden y deben contribuir a la prevención a través del compromiso decidido de sus líderes para establecer una cultura de integridad, transparencia, honestidad, cumplimiento y de lucha contra el soborno y la corrupción. En este sentido, existe la Certificación Anti-Soborno, uno de lo requisitos más solicitados por las compañías de la región, emitido por el Sistema de Gestión Anti-Soborno (SGAS).

El mismo se encuentra regulado por la norma **ISO 37.001:2017**: un reconocido estándar internacional en la materia que guía a las organizaciones en el establecimiento, implementación y mantenimiento de un sistema de gestión con este propósito, ya que les ofrece una serie de medidas que podrán adoptar, de forma proporcional y razonable, para prevenir, detectar y gestionar conductas delictivas de soborno cumpliendo con la legislación y con otros compromisos adquiridos de forma voluntaria. Esta norma es aplicable en cualquier organización a nivel global, sin importar su tamaño, actividad ni sector, tampoco si es gubernamental, privada o sin fines de lucro.

Someter los procesos de trabajo bajo la Gestión Anti-Soborno impacta positivamente en las organizaciones ya que promueve:

- Demostración de compromiso con la integridad y ética en los negocios.
- Establecimiento de políticas y procedimientos sólidos para prevenir y mitigar el soborno.
- Reducción del riesgo de conductas ilícitas y protección de la reputación de la organización.
- Generación de confianza entre clientes, socios comerciales y partes interesadas.
- Cumplimiento de estándares rigurosos de transparencia y legalidad.
- Atracción de nuevas oportunidades comerciales basadas en la confianza y la integridad.
- Claro compromiso con la honestidad, la responsabilidad y la transparencia.
- Aporte de valor adicional en términos de reputación y oportunidades de negocio.

> “Esta norma regula la actividad de toda nuestra compañía y es la forma más transparente de hacer negocios con nuestros clientes.”

Andrés Quinn
COO de OCP TECH

Conoce más sobre esta noticia en:
Una empresa latinoamericana fue la primera en la región en recibir una certificación anti-soborno

IDENTIDAD DIGITAL

LA CONTRASEÑA ¿HA MUERTO?

Nuevas formas de identificación promueven el fin de las contraseñas. ¿Cómo podemos validar hoy nuestro ser de forma única, privada y segura?

El futuro nos ofrece oportunidades y desafíos. Actualmente el ecosistema digital propone, tanto a las organizaciones como a los individuos, modificar constantemente sus dinámicas, actualizarse y afrontar una vida digital que plantea mejoras y a su vez, retos cibernéticos.

Hasta hace poco, con el objetivo de proteger transacciones, activos, información, el camino del usuario recorría, sí o sí, una primera barrera de protección básica: la contraseña. La consigna impone generar contraseñas que combinen números y caracteres, mayúsculas y minúsculas, con determinada cantidad de dígitos; cambiarlas periódicamente, jamás guardarlas en un archivo ubicado en la nube y menos compartirlas con alguien; contar con contraseñas diferentes para cada aplicación. Algunas empresas utilizan un generador de contraseñas, con la intención de crear contraseñas más complejas y seguras. El modelo de las claves y las contraseñas es sinónimo de una constante autenticación para demostrar que verdaderamente somos nosotros.

Entonces aparece en escena el concepto de Identidad Digital Única, es decir, un sistema de identificación efectivo y seguro, a tono con la transformación digital que vienen asumiendo organizaciones y usuarios, con conexiones rápidas y eficientes, que utilizan las tecnologías más avanzadas del mercado.

Toda transacción o interacción se procesa a través de la identidad, y en tiempos más próximos que futuros, será natural una autenticación sin contraseñas.

Elegir el nuevo camino

El tiempo de la autenticación sin contraseña no sólo ha llegado, sino que potencia la seguridad y garantiza una mejor experiencia del cliente.

Los métodos de autenticación sin contraseñas son variados.

Un ejemplo es la autenticación biométrica, que verifica la identidad de un usuario utilizando características físicas o de comportamiento. Puede ser por reconocimiento de voz, facial o de huellas dactilares, por escaneo de iris. La biometría se utiliza cada vez más en las aplicaciones. A diferencia de las contraseñas, los datos biométricos no se pueden olvidar ni compartir y son más difíciles de copiar o robar.

El método Single-Sign-On (SSO) permite al usuario iniciar sesión de forma segura en aplicaciones de terceros utilizando un único conjunto de credenciales. Se realiza iniciando sesión, por ejemplo, con servicios de Google, Microsoft o Facebook. El SSO busca simplificar la experiencia de los usuarios en Internet facilitando las tareas de inicio de sesión completamente.

Los Factores de Posesión, por su parte, otorgan acceso a los usuarios a través de un dispositivo móvil o algo que poseen, como determinada identificación. Se recibe un código de acceso único (OTP) por correo electrónico o SMS, se inicia sesión en el sistema automáticamente respondiendo a las notificaciones o ingresando los códigos.

Los Enlaces Mágicos son otra forma de autenticación sin contraseña. Se realiza a través del envío de una URL única al correo electrónico del usuario, quien puede iniciar sesión en la aplicación o cuenta. Por razones de seguridad, tienen una duración limitada y son únicos, lo que significa que no son válidos después de un tiempo determinado.

Animarse al cambio

Todos los años, los investigadores estudian cuáles son las contraseñas más comunes, y observan que, a pesar de la creciente concientización sobre la ciberseguridad, se repiten sistemáticamente. Los usuarios siguen usando contraseñas débiles para proteger sus cuentas y datos. Por otra parte, las contraseñas son el objetivo más común de los ataques. Los ciberdelincuentes utilizan el *phishing* y el método de fuerza bruta para

obtenerlas, lo que significa que también pueden acceder a datos confidenciales de las personas y las empresas.

Hoy, los métodos de autenticación sin contraseña pueden mejorar la experiencia del usuario, y también optimizar costos, reducir las filtraciones de datos y alcanzar mayor productividad de la fuerza laboral de las organizaciones.

El desafío para su implementación comienza por aceptar el cambio y evaluar las mejores soluciones que brinda la tecnología de autenticación sin contraseña, sus características y seguridad.

MIA Identidad Digital Única

Estas son algunas de las características más relevantes de la plataforma de OCP TECH, que garantiza un proceso de autenticación simple y seguro, sin contraseñas:

- Es omnicanal e interoperable: respeta los estándares internacionales en materia de tratamiento de los datos y seguridad.

- Ofrece un modelo de interacción independiente del canal o el dispositivo, con certificación FIDO de punta a punta.

- Las transacciones se autentican por medio de múltiples factores biométricos, a elección del usuario. Esto elimina la necesidad de utilizar usuarios y contraseñas, así como los modelos tradicionales de segundo factor, por ejemplo la validación de un correo o número telefónico. Asimismo, se reduce el riesgo de fraude y la fricción: no se altera el flujo o la experiencia, y tampoco es necesario generar descargas adicionales en otras aplicaciones, ni tareas complejas.

- Cuanto más se utiliza más se fortalece, a diferencia del modelo del usuario y contraseña, que cuanto más se usa más se debilita, porque más se expone.

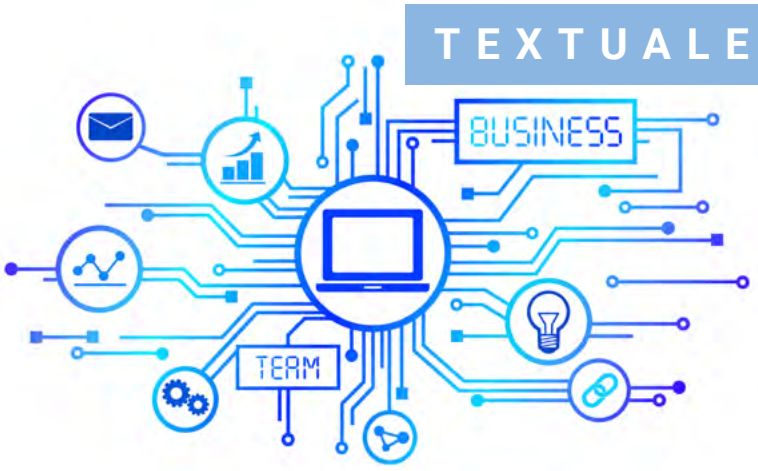
- Respeta la privacidad, ya que el usuario no necesita exponer más información que la necesaria.

- La información es inmutable, nadie la puede vulnerar, los datos son soberanos, se utiliza un algoritmo específico que transforma a la experiencia en simple y segura.

- En Argentina, MIA está integrada con el Registro Nacional de las Personas, con la aplicación Nosis, con la Administración Federal de Ingresos Públicos.

2 preguntas

Dos referentes del mercado de tecnología brindan su punto de vista acerca de cómo ésta contribuye al mejor desempeño de las organizaciones.



Andrés López

Secretario TIC, Gobernación Antioquia

¿Cómo impacta la tecnología en el desarrollo de una organización?

Contribuye en la eficiencia operativa, facilita la comunicación y colaboración interna, permite llegar a nuevos mercados, mejorar la experiencia del cliente y facilitar el análisis de datos para la toma de decisiones. Los puntos claves a tener en cuenta en la actualidad tienen que ver con:

Ciberseguridad: implementar medidas de seguridad como *firewalls*, antivirus y sistemas de detección y respuesta ante incidentes (EDR) a la vez que se educa a los usuarios sobre las mejores prácticas y se promueve la conciencia sobre las técnicas utilizadas por los ciberdelincuentes.

Infraestructura tecnológica: buscar su solidez a través de servidores, redes, almacenamiento en la nube y otros componentes necesarios para respaldar las operaciones empresariales.

Data: a partir de su importancia y valor, es imprescindible implementar políticas adecuadas para el manejo seguro de datos, el cifrado de información sensible y la realización regular de copias de seguridad para evitar pérdidas o daños.

Identidad digital: su gestión adecuada implica asegurar que sólo las personas autorizadas tengan acceso a sistemas y datos confidenciales mediante métodos avanzados de autenticación.

Análisis de datos: una buena gestión incluye contar con capacidad para recopilar grandes volúmenes de datos, utilizar herramientas analíticas avanzadas como IA o aprendizaje automático, así como garantizar la privacidad y cumplimiento normativo al manejarlos.

¿Qué opinas respecto de las tecnologías de la industria 4.0 y su impacto social?

La Inteligencia Artificial, el Internet de las Cosas y la Automatización, tienen un gran potencial para transformar la sociedad y mejorar la eficiencia en diversos sectores industriales, pues pueden aumentar la productividad, reducir costos y mejorar la calidad de vida de las personas al facilitar tareas cotidianas y permitir una mayor conectividad. Además, pueden generar nuevos empleos y oportunidades económicas. Sin embargo, es importante considerar sus posibles impactos sociales: el reemplazo de empleos por automatización y cómo esto puede afectar a ciertos sectores de la población, la privacidad y seguridad de los datos, entre otros.

Santiago Ezequiel Edreira

Gerente corporativo Gestión de Servicios de TI, Grupo Arcor

¿Cuáles son los beneficios de la tecnología en una organización?

En términos generales, su impacto brinda beneficios clave que impulsan el crecimiento y la eficiencia. Aporta agilidad, flexibilidad y adaptabilidad para afrontar un cambiante contexto de negocios, mejora el proceso de toma de decisiones y es, además, el factor distintivo para afrontar la transformación digital. Hoy, todo dentro de una organización está impactado y/o apalancado en la tecnología. Ya no existen los procesos de negocio por un lado y los tecnológicos por el otro: todo proceso de negocio va acompañado del desarrollo tecnológico y todo proceso tecnológico tiene un fin de negocios. Como ejemplo puedo citar las soluciones de colaboración, como Cisco Webex, que desempeñan un papel crucial al mejorar la comunicación y eficiencia dentro de la organización.

¿Qué opinión tienes respecto a las nuevas tecnologías y su impacto social?

La tecnología, bien utilizada, tiene el potencial de facilitarle la vida a la gente y mejorar la integración de empresas con sus entornos, aunque del mismo modo, puede dañar un ecosistema. Es importante que siempre estén bien utilizadas y que los marcos regulatorios sean claros.

Futuro y presente de las **Smart Cities**

Las Smart Cities o Ciudades Inteligentes son aquellas en las que se aplican las tecnologías de la información y de las comunicaciones (TIC), con el objetivo de dotarlas de infraestructuras que garanticen o faciliten su funcionamiento. Un desarrollo sostenible, mejor calidad de vida y una mayor eficacia y eficiencia en el uso de los recursos disponibles son parte de los increíbles beneficios que las Smart Cities entregan a todos los ciudadanos.

por **Freddy Macho**
Presidente del Centro de Investigación de Ciberseguridad del IoT – IIoT
Presidente del Comité IoT del Laboratorio de Ciberseguridad (OEA)
Coordinador Regional del Centro de Ciberseguridad Industrial de España (CCI)
Expert Researcher ICS – IoT – IIoT (Global Foundation for Cyber Studies and Research)
Presidente del IoT Security Institute, capítulo Chile (IoTSI)
Asesor de Ciberseguridad – Junta de Directorio Holding

Respuesta al desafío de una población creciente

Una tendencia que parece imparable es la disolución de los límites entre el ciberespacio y el mundo físico. Una expresión de esta integración es el Internet de las Cosas (Internet of Things, IoT) y la proliferación de aparatos conectados a la red, que va mucho más allá de los *smartphones* o los electrodomésticos inteligentes. El Internet de las Cosas es un nuevo cambio de paradigma en el mundo de la tecnología de la información (TI), donde las cosas tienen identidades digitales, funcionalidades con inteligencia artificial (IA) y que se pueden ubicar, rastrear, monitorear, controlar y automatizar. La aceleración hacia la digitalización y el trabajo remoto han impulsado que el uso de la hiperconvergencia se incremente con enorme rapidez.

La población mundial está creciendo de manera sostenida y según estudios de las Naciones Unidas, aproximadamente 83 millones de personas se agregan cada año. Se estima que actualmente el número de habitantes a nivel global es de 7.300 millones personas y que alcanzará los 9.700 millones para el año 2050. De igual manera, el Departamento de Asuntos Económicos y Sociales de las Naciones Unidas ha lanzado un documento que prevé que el 68 % de la población vivirá en zonas urbanas de cara a 2050, lo cual representa un enorme desafío para entregar servicios eficientes a un número enorme de habitantes en zonas altamente reducidas.

Debido a esta realidad, el manejo de conceptos tales como la eficiencia energética, el desarrollo sustentable y la protección del medio ambiente, la reducción de las emisiones de CO2 que se envían a la atmósfera, la descarbonización, la eliminación progresiva del consumo de combustibles fósiles, el control del consumo de la demanda hídrica, entre otros puntos, son imprescindibles para facilitar un adecuado nivel de vida a los habitantes de las futuras zonas urbanas a nivel global.

Cuando se habla de que una ciudad es inteligente se está destacando que es capaz de desarrollar un proceso de planificación estratégica sólido que, en base a las necesidades y oportunidades propias de la zona, permite establecer sus prioridades y ser lo suficientemente flexible para adaptarse a los cambios que vienen de la mano con la sobrepoblación de las ciudades y las potentes señales del cambio climático.

Por otro lado, cada ciudad tiene sus propios problemas y ritmo de crecimiento. Las consecuencias positivas y negativas producto del aumento de la población impactan en distintos grados, por lo que la estrategia necesaria para preparar la ciudad del futuro transformándola en una ciudad inteligente es única para la zona y su comunidad. Trabajar para lograr una ciudad inteligente implica la colaboración del sector público y privado, donde toda la comunidad debe ser y sentirse parte del cambio: ciudadanos, organizaciones, empresas, Gobierno, centros de investigación, universidades, etc., todos funcionando en perfecta armonía como un ecosistema de la naturaleza.

Dentro del espectro de ámbitos que intervienen en el desafío de formar ciudades inteligentes, al menos deben considerarse los siguientes:

- Las tecnologías habilitadoras
- Movilidad
- Vida e Inclusión
- Infraestructuras y edificios
- Ciberseguridad y Seguridad Pública
- Economía
- Educación
- Energía
- Medio ambiente y cambio climático
- Finanzas
- Incendios y respuesta a las emergencias
- Gobernanza
- Salud
- Vivienda
- Población y condiciones sociales
- Recreación
- Seguridad
- Residuos sólidos
- Deporte y cultura
- Telecomunicaciones
- Planificación urbana
- Transporte
- Agricultura urbana/local y seguridad alimentaria
- Aguas residuales
- Agua
- Post-pandemia

El despliegue del IoT plantea muchos problemas de ciberseguridad derivados de la propia naturaleza de los objetos inteligentes, por ejemplo, la adopción de algoritmos criptográficos ligeros, en términos de requisitos de procesamiento y memoria, y el uso de protocolos estándar, así como la necesidad de minimizar la cantidad de datos que pudieran quedar expuestos en el intercambio entre nodos. La integración del mundo físico en el tejido de la web impone requisitos de ciberseguridad avanzados que deben satisfacerse para garantizar un control estricto sobre la interacción de los servicios en el IoT.

Smart Cities y Ciberseguridad

Las ciudades inteligentes mejoran la calidad de vida de los ciudadanos en lo que respecta al uso de la energía y el agua, la atención sanitaria, el impacto medioambiental, las necesidades de transporte, las necesidades de seguridad pública (física -delincuencia tradicional, y lógica -ciberdelincuencia), y muchos otros servicios esenciales de la ciudad. Los recientes avances en *hardware* y *software* han impulsado el rápido crecimiento y despliegue de la conectividad ubicua entre los componentes físicos y cibernéticos de una ciudad, en particular con el advenimiento de los dispositivos IoT y el despliegue de las tecnologías 5G. Sin embargo, esta conectividad también abre muchas puertas para la ciberdelincuencia que se expresan a través de vulnerabilidades de ciberseguridad que deben ser conocidas y comprendidas por los usuarios con miras a su correcta mitigación.

Una mirada integradora y moderna de las ciudades inteligentes no puede dejar atrás conceptos tan críticos hoy en día como medio ambiente, sostenibilidad y seguridad. No se trata sólo de aumentar la tecnología ni de hacer más eficientes los servicios para los habitantes de las ciudades; hay que velar por que éstos se brinden con criterios de respeto al entorno y resguardando los derechos humanos y la ciberseguridad de los ciudadanos.

Oportunidades para los ciberdelincuentes

En esta vorágine de tecnologías aplicadas a mejorar el vivir dentro de las ciudades, indudablemente la interacción entre diversos actores y el intercambio de datos son elementos relevantes para poder accionar estas tecnologías, actividades o procesos. Debido a esta condición, algunas oportunidades que pueden encontrar los ciberdelincuentes son:

- Ciberseguridad pobre o inexistente, tanto a nivel general como particular. El nivel de seguridad de un sistema lo marca su elemento más desprotegido.
- Proveedores de tecnología que dificultan o imposibilitan la investigación en ciberseguridad.
- Complejidad excesiva de los sistemas y las plataformas, que dificulta localizar un ataque y frenarlo.
- Falta de evaluaciones de seguridad sobre dichos sistemas, plataformas y tecnologías.
- Sistemas heredados con baja seguridad como, por ejemplo, plataformas, *software* que no se actualiza o tecnologías en las que es imposible implementar sistemas de cifrado.
- Susceptibilidad a ataques DoS o de denegación de servicio, con múltiples agresiones dirigidas a un mismo punto con el objetivo de dejarlo inoperativo. Las embestidas podrían incluso generarse desde los propios objetos conectados de la ciudad o, al menos, desde aquellos con una seguridad deficiente.
- Riesgos derivados de un funcionamiento inadecuado de la administración para gestionar los retos de las ciudades conectadas.
- Ausencia o elaboración pobre de planes de emergencia contra ciberataques y carencia de equipos de respuesta a incidentes.

Problemas de ciberseguridad, que se visualizan:

- La mayoría de las ciudades alrededor del mundo están implementando nuevas

- tecnologías sin primero probar su ciberseguridad.

- No están considerando prácticas de seguridad básicas en las tecnologías desplegadas.

- La mayoría de las tecnologías son inalámbricas, las cuales son fácilmente *hackeables* si no se utilizan controles de encriptación adecuados.

- La mayoría de las ciudades no cuentan con CERT/CSIRT que ayuden a coordinar la respuesta ante incidentes de ciberseguridad.

- Resulta ser una práctica habitual que las ciudades utilicen tecnologías vulnerables debido a que los fabricantes son lentos para liberar los parches de seguridad o éstos no son aplicados.

- En general les resulta difícil a las ciudades dejar de utilizar sistemas antiguos y vulnerables; éstos agregan complejidad e incrementan la superficie de ataque.

- Las ciudades no tienen planes de emergencia ante ataques, lo que implica que no están preparadas para enfrentar un ciberataque.

- El uso de la tecnología genera dependencia en las ciudades y puede ser explotada por atacantes que atenten contra los pilares de la ciberseguridad: confidencialidad, integridad y disponibilidad.

Mejores prácticas de ciberseguridad para ciudades inteligentes

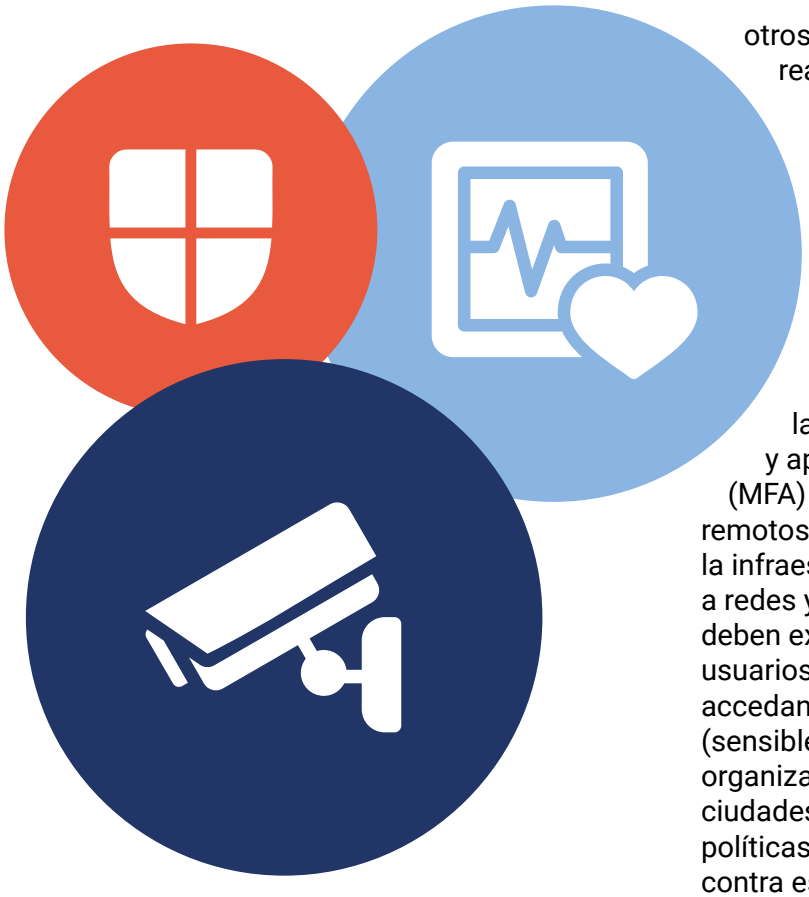
La integración de los servicios públicos en un entorno conectado puede aumentar la eficiencia y la resiliencia de la infraestructura que sustenta la vida cotidiana en nuestras comunidades. Sin embargo, las comunidades que estén considerando convertirse en ciudades inteligentes deben evaluar y mitigar minuciosamente el riesgo de ciberseguridad que conlleva esta integración. Las ciudades inteligentes son *targets* atractivos para ciberataques maliciosos debido a:

- Los datos que se recopilan, transmiten, almacenan y procesan, que pueden incluir cantidades significativas de información confidencial de gobiernos, empresas y ciudadanos privados.

- Los complejos sistemas de *software* impulsados por inteligencia artificial, que pueden tener vulnerabilidades y que las ciudades inteligentes a veces utilizan para integrar los datos.

Recomendaciones

Las comunidades deben garantizar que cualquier característica “inteligente” o conectada que planeen incluir en la nueva infraestructura sea segura por diseño e incorpore conectividad segura con cualquier sistema heredado restante. Asimismo, deben ser conscientes de que la infraestructura heredada puede requerir un rediseño para implementar de forma segura sistemas de



ciudades inteligentes. La planificación de la seguridad debe centrarse en crear resiliencia a través de una defensa en profundidad y tener en cuenta tanto el riesgo físico como el cibernético, así como el entorno ciberfísico convergente que introducen los sistemas IoT e IoT industrial (IIoT).

Aplicar el principio de privilegio mínimo

Las organizaciones responsables de implementar la tecnología de ciudades inteligentes deberían aplicar el principio de privilegio mínimo en todos sus entornos de red. Según lo define el Instituto Nacional de Estándares y Tecnología (NIST) de EE. UU., el principio de privilegio mínimo es: "El principio de que una arquitectura de seguridad debe diseñarse de modo que a cada entidad se le otorguen los recursos mínimos del sistema y las autorizaciones que la entidad necesita para realizar sus tareas y cumplir su función." Los administradores deben revisar las configuraciones predeterminadas y existentes junto con las pautas de refuerzo de los proveedores para garantizar que el *hardware* y el *software* sólo tengan permiso para acceder a otros sistemas y datos que necesitan para realizar sus funciones.

Aplicar la autenticación multifactor

Las organizaciones responsables de implementar la tecnología de ciudades inteligentes deben proteger las aplicaciones de acceso remoto y aplicar la autenticación multifactor (MFA) en cuentas y dispositivos locales y remotos cuando sea posible para fortalecer la infraestructura que permite el acceso a redes y sistemas. Las organizaciones deben exigir explícitamente MFA cuando los usuarios realicen acciones privilegiadas o accedan a repositorios de datos importantes (sensibles o de alta disponibilidad). Las organizaciones responsables de implementar ciudades inteligentes deben revisar las políticas de configuración para protegerse contra escenarios de "falla de apertura" y reinscripción.

Implementar una arquitectura de confianza cero

La implementación de principios de diseño de red de confianza cero creará un entorno de red más seguro que requiere autenticación y autorización para cada nueva conexión con un enfoque de seguridad de defensa en profundidad en capas. La confianza cero también permite una mayor visibilidad de la actividad de la red, la identificación de tendencias mediante análisis, la resolución de problemas mediante la automatización y la orquestación, y una gobernanza de la seguridad de la red más eficiente.

Gestionar cambios en los riesgos de la arquitectura interna

Las organizaciones responsables de implementar la tecnología de ciudades inteligentes deben comprender su entorno y gestionar cuidadosamente las

comunicaciones entre subredes, incluidas las subredes recientemente interconectadas que vinculan sistemas de infraestructura. Los administradores de red deben estar conscientes de la evolución de su arquitectura de red y del personal responsable de la seguridad del conjunto integrado y de cada segmento individual. Los administradores deben identificar, agrupar y aislar los sistemas comerciales críticos y aplicar los controles de seguridad de red y los sistemas de monitoreo adecuados para reducir el impacto de un compromiso en toda la comunidad.

Administrar de forma segura los activos de la ciudad inteligente

Implica proteger los activos de la ciudad inteligente contra robos y cambios físicos no autorizados, así como considerar implementar controles de seguridad físicos y lógicos para proteger sensores y monitores contra manipulación, robo, vandalismo y amenazas ambientales.

Parchear sistemas y aplicaciones de manera oportuna

Cuando sea posible, habilite procesos de parcheo automáticos para todos los dispositivos de *software* y *hardware* que incluyan validación de autenticidad e integridad. Aproveche la inteligencia sobre amenazas para identificar amenazas activas y garantizar que los sistemas y la infraestructura expuestos estén protegidos. Proteja los activos de *software* a través de un programa de gestión de activos que incluya un proceso del ciclo de vida del producto. Este proceso debe incluir la planificación de reemplazos para componentes y *software* que se acercan o han superado el final de su vida útil, ya que los fabricantes o desarrolladores pueden dejar de crear parches.

Revisar los riesgos legales, de seguridad y de privacidad asociados con las implementaciones

Implemente procesos que evalúen y gestionen continuamente los riesgos legales y de privacidad asociados con las soluciones implementadas.

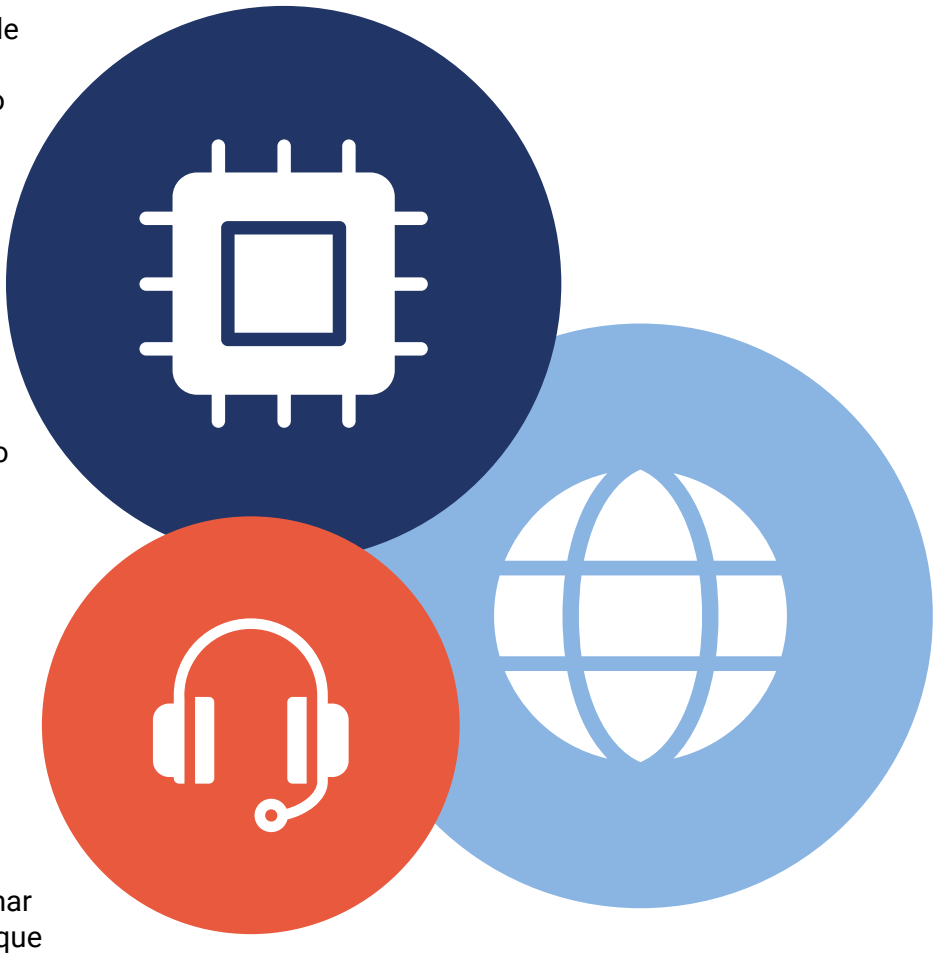
Gestionar proactivamente los riesgos en la cadena de suministro

Todas las organizaciones responsables de implementar tecnología de ciudades inteligentes deben gestionar de manera proactiva el riesgo de la cadena de suministro de TIC para cualquier tecnología nueva, incluido el *hardware* o *software* que respalda la implementación de sistemas de ciudades inteligentes o proveedores de servicios que respaldan la implementación y las operaciones. Las organizaciones deben utilizar únicamente proveedores y componentes de TIC confiables. El proceso de gestión de riesgos de la cadena de suministro de TIC debe incluir la participación de todos los niveles de la organización y contar con el apoyo total de los líderes de programas que implementan sistemas de ciudades inteligentes.

Cadena de suministro de *software*

Las organizaciones responsables de implementar la tecnología de ciudades inteligentes deben establecer requisitos o controles de seguridad para los proveedores de *software* y garantizar que los proveedores

potenciales utilicen un ciclo de vida de desarrollo que incorpore prácticas seguras, mantenga un proceso activo de identificación y divulgación de vulnerabilidades y permita la gestión de parches. Los proveedores de productos también deberían asumir parte del riesgo asociado con sus productos y desarrollar tecnología de ciudad inteligente respetando los principios de seguridad por diseño y seguridad por defecto y el mantenimiento activo de los productos que ofrecen.



Cadena de suministro de *hardware* y dispositivos IoT

Las organizaciones responsables de implementar la tecnología de ciudades inteligentes deben determinar si los dispositivos y *hardware* de IoT que permitirán la funcionalidad "inteligente" requerirán soporte de servicios externos o de terceros. Estas organizaciones deben realizar investigaciones minuciosas sobre cómo se obtienen y ensamblan las piezas para crear productos. También deben determinar cómo los dispositivos almacenan y comparten datos y cómo protegen los datos en reposo, en tránsito y en uso. Las organizaciones deben mantener un registro de riesgos que identifique su propia dependencia y la de sus proveedores en el soporte de computación en la nube, componentes de origen externo y dependencias similares.

Proveedores de servicios gestionados y proveedores de servicios en la nube

Las organizaciones deben establecer requisitos de seguridad claros para los proveedores de servicios gestionados y otros proveedores que respaldan la implementación y las operaciones de tecnología de ciudades inteligentes. Asimismo, deben tener en cuenta los riesgos de contratar proveedores externos en su planificación general de gestión de riesgos y garantizar que los estándares de seguridad organizacional se incluyan en los acuerdos contractuales con partes externas. De manera similar, las organizaciones deben revisar cuidadosamente los acuerdos de servicios en la nube, incluidas las disposiciones de seguridad de los datos y los modelos de responsabilidad compartida.

Resiliencia operativa

Las organizaciones responsables de implementar la tecnología de ciudades inteligentes deben desarrollar, evaluar y mantener contingencias para las operaciones manuales de todas las funciones críticas de la infraestructura y capacitar al personal en consecuencia. Esas contingencias deberían incluir planes para desconectar los sistemas de infraestructura entre sí o de la Internet pública para operar de forma autónoma. En caso de que se produzca un compromiso, las organizaciones deben estar preparadas para aislar los sistemas afectados y operar otra infraestructura con la menor interrupción posible.

Sistemas de respaldo y datos

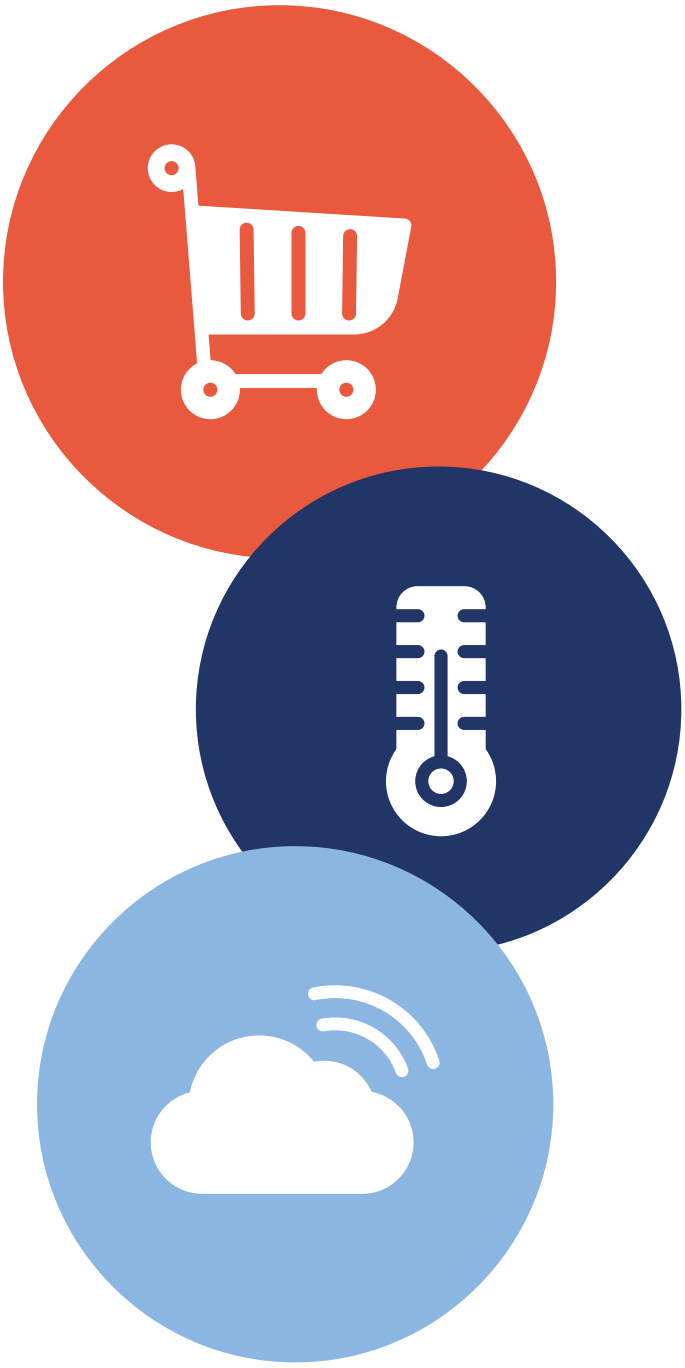
Las organizaciones responsables de implementar la tecnología de ciudad inteligente deben crear, mantener y probar copias de seguridad, tanto para los registros del sistema de TI como para las capacidades operativas manuales de los sistemas físicos integrados en una red de ciudad inteligente. Estas organizaciones deben identificar cómo y dónde se recopilarán, procesarán, almacenarán y transmitirán los datos y garantizarán que cada nodo de ese ciclo de vida de los datos esté protegido. Los administradores de sistemas deben almacenar las copias de seguridad de TI por separado y aislarlas para inhibir la propagación del *ransomware* ya que muchas de sus variantes intentan encontrar y cifrar o eliminar las copias de seguridad accesibles. Aislar las copias de seguridad permite restaurar los sistemas/datos a su estado anterior en caso de un ataque de este tipo.

Realizar capacitación de la fuerza laboral

Aunque la implementación de tecnología de ciudad inteligente puede incluir una amplia automatización, los empleados responsables de gestionar las operaciones de infraestructura deben estar preparados para aislar los sistemas de TI comprometidos de la OT y operar manualmente las funciones principales si es necesario. Las organizaciones deben capacitar a los empleados nuevos y existentes en operaciones integradas y automatizadas, así como en procedimientos de respaldo manuales aislados, incluidos procesos para restaurar el servicio después de un reinicio. Las organizaciones deben actualizar la capacitación periódicamente para tener en cuenta las nuevas tecnologías y componentes.

Desarrollar y ejercitar planes de respuesta y recuperación ante incidentes

Los planes de respuesta y recuperación ante incidentes deben contener roles y responsabilidades para todas las partes interesadas, incluidos líderes ejecutivos, líderes técnicos y oficiales de adquisiciones dentro y fuera del equipo de implementación de la ciudad inteligente. Las organizaciones responsables de implementar la tecnología de Smart Cities deben mantener copias impresas actualizadas y accesibles de estos planes para los socorristas en caso de que la red sea inaccesible (por ejemplo, debido a un ataque de *ransomware*). Las organizaciones deben ejercitar sus planes anualmente y coordinarse internamente para garantizar la continuidad de las operaciones.



Producción Integral
Basanta Contenidos

Directora Editorial
Karina Basanta

Director de Arte
Nicolás Cuadros

Coordinadores
Marta Azzani
Emiliano Martínez

Producción audiovisual
Salpufilms

Colaboran en este número
Silvia Montenegro

Fotografía e ilustración
Basanta Contenidos
Santiago Guerrero
Freepik

Traducción
María Gimena González Marino

Agradecimientos
Claudia Menkarsky
Freddy Macho
Pablo Marrone
Eric Balderrama

Basanta contenidos

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

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


OCP TECH
INGENIERÍA DE IMPACTO
@somosOCPTECH
ocp.tech
/ocp-tech
@OCPTECH